

Información Importante

La Universidad Santo Tomás, informa que el(los) autor(es) ha(n) autorizado a usuarios internos y externos de la institución a consultar el contenido de este documento a través del catálogo en línea, página web y Repositorio Institucional del CRAI-USTA, así como en las redes sociales y demás sitios web de información del país y del exterior con las cuales tenga convenio la Universidad.

Se permite la consulta a los usuarios interesados en el contenido de este documento, para todos los usos que tengan **finalidad académica**, siempre y cuando mediante la correspondiente cita bibliográfica se le dé crédito al trabajo de grado y a su autor, nunca para usos comerciales.

De conformidad con lo establecido en el Artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, la Universidad Santo Tomás informa que “los derechos morales sobre documento son propiedad de los autores, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.”

Centro de Recursos para el Aprendizaje y la Investigación, CRAI-USTA

Universidad Santo Tomás, Bucaramanga

**Medición del Riesgo Operativo en una Sucursal Bancaria de la Ciudad de
Bucaramanga, una Aplicación de Redes Bayesianas**

Jersson Reynaldo Suarez Jiménez

Trabajo de grado para optar al título de Ingeniero Industrial

Director

Msc.Javier Hernández Cáceres

Docente-Investigador

Universidad Santo Tomás, Bucaramanga

División de Ingenierías y Arquitectura

Facultad de Ingeniería Industrial

2021

Contenido

| | |
|--|----|
| Introducción | 12 |
| 1. Definición del Problema | 13 |
| 1.1 Descripción del Problema | 13 |
| 1.2 Formulación del Problema..... | 15 |
| 1.3 Justificación | 15 |
| 1.4 Alcance | 17 |
| 2. Objetivos | 18 |
| 2.1 Objetivo General | 18 |
| 2.2 Objetivos Específicos..... | 19 |
| 3. Marco Referencial..... | 19 |
| 3.1 Marco Teórico..... | 19 |
| 3.1.1 Redes Bayesianas | 19 |
| 3.1.2 Conceptos para la Comprensión del Teorema de Bayes | 21 |
| 3.1.3 Fundamentación de las Redes Bayesianas | 22 |
| 3.1.4 Tipos de Redes Bayesianas | 25 |
| 3.1.5 Inferencia Bayesiana | 26 |
| 3.1.6 Simulación Estocástica | 31 |
| 3.1.7 Algoritmo de Condicionamiento..... | 31 |
| 3.2 Marco Conceptual | 32 |
| 3.3 Marco Histórico | 34 |
| 3.4 Marco Normativo | 36 |

| | |
|--|----|
| 3.5 Estado del Arte..... | 37 |
| 4. Metodología | 44 |
| 4.1 Tipo de Estudio..... | 44 |
| 4.2 Fases de la Investigación..... | 45 |
| 4.2.1 Fase 1..... | 45 |
| 4.2.2 Fase 2..... | 46 |
| 4.2.3 Fase 3..... | 46 |
| 4.2.4 Fase 4..... | 47 |
| 4.2.5 Fase 5..... | 47 |
| 4.2.6 Fase 6..... | 47 |
| 4.2.7 Fase 7..... | 48 |
| 5. Análisis e Interpretación de Resultados | 48 |
| 5.1 Caracterización de la Línea de Negocio Objeto de Estudio..... | 49 |
| 5.2 Categorización de posibles eventos de pérdidas identificados | 51 |
| 5.2.1 Fraude Interno | 51 |
| 5.2.2 Fraude Externo..... | 51 |
| 5.2.3 Fallas en los Sistemas e Interrupción del Negocio | 51 |
| 5.2.4 Manejo y Ejecución de Procesos | 52 |
| 5.3 Niveles de Severidad para Posibles Eventos de Pérdida..... | 52 |
| 5.4 Indicadores de Riesgo Operativo Identificados | 52 |
| 5.4.1 Categoría Fraude Interno | 53 |

| | |
|--|-----|
| 5.4.2 Categoría Fraude Externo | 55 |
| 5.4.3 Categoría Fallas en los Sistemas e Interrupción del Negocio | 56 |
| 5.4.4 Categoría Manejo y Ejecución de Procesos | 58 |
| 5.5 Modelo de Red Bayesiana propuesto para la Sucursal Bancaria Objeto de Análisis | 59 |
| 5.5.1 Categoría Fraude Interno | 59 |
| 5.5.2 Categoría Fraude Externo | 67 |
| 5.5.3 Categoría Fallas en los Sistemas e Interrupción del Negocio | 70 |
| 5.5.4 Categoría Manejo y Ejecución de Procesos | 73 |
| 5.6 Validación de Modelo de Red de Bayesiana | 76 |
| 5.7 Distribución de Pérdidas agregadas | 76 |
| 5.7.1 Ajuste de Distribución de Severidad de la Categoría Fraude Interno | 78 |
| 5.7.2 Ajuste de Distribución de Severidad de la Categoría Fraude Externo | 81 |
| 5.7.3 Ajuste de Distribución de Severidad de la Categoría Manejo de Procesos | 84 |
| 6. Conclusiones | 92 |
| 7. Recomendaciones | 93 |
| Referencias | 94 |
| Apéndices | 101 |

Lista de Tablas

| | Pág. |
|--|-------------|
| Tabla 1. <i>Normas</i> | 36 |
| Tabla 2. <i>Probabilidades condicionales para el nodo entrega segura de claves</i> | 59 |
| Tabla 3. <i>Probabilidades para Personas que intervienen en la creación de claves</i> | 60 |
| Tabla 4. <i>Probabilidades para Recepción segura de claves por clientes</i> | 61 |
| Tabla 5. <i>Probabilidades para Personal con antecedentes disciplinarios</i> | 61 |
| Tabla 6. <i>Probabilidades para Nivel de vida del personal</i> | 62 |
| Tabla 7. <i>Probabilidades para Supervisión</i> | 63 |
| Tabla 8. <i>Probabilidades para Manejo seguro de la información de clientes</i> | 63 |
| Tabla 9. <i>Probabilidades para Nivel de restricción para pagos a terceros</i> | 64 |
| Tabla 10. <i>Probabilidades para control del sistema central por parte del superusuario para crear, editar y eliminar usuarios</i> | 67 |
| Tabla 11. <i>Probabilidades para control del sistema central por parte del superusuario para manipular datos contenidos en archivos de pagos a terceros</i> | 68 |
| Tabla 12. <i>Probabilidades a priori de disponibilidad de firewall</i> | 70 |
| Tabla 13. <i>Probabilidades a priori para nivel concurrencia del servidor</i> | 71 |
| Tabla 14. <i>Probabilidades a priori del nivel de calidad del hardware</i> | 71 |
| Tabla 15. <i>Probabilidades para envío de claves vía e-mail</i> | 73 |
| Tabla 16. <i>Probabilidades a priori para envío de claves vía teléfono</i> | 73 |
| Tabla 17. <i>Probabilidades condicionales para nodo errores en el registro de clientes</i> | 74 |
| Tabla 18. <i>Pronóstico del riesgo operativo resultante</i> | 91 |

Lista de Figuras

| | Pág. |
|---|-------------|
| Figura 1. <i>Flujograma para construir una Red Bayesiana</i> | 24 |
| Figura 2. <i>Red Bayesiana Dinámica. Representación de una Red Bayesiana Dinámica</i> | 26 |
| Figura 3. <i>Ejemplo de estructura de una Red Bayesiana</i> | 29 |
| Figura 4. <i>Red Bayesiana para fraude interno</i> | 66 |
| Figura 5. <i>Red Bayesiana para fraude externo</i> | 69 |
| Figura 6. <i>Red Bayesiana para fallas en sistema e interrupción del negocio</i> | 72 |
| Figura 7. <i>Red Bayesiana de manejo y ejecución de procesos</i> | 75 |
| Figura 8. <i>P-value para distribución fraude interno</i> | 79 |
| Figura 9. <i>Distribución de datos de severidad ajustada a la distribución Lognormal para fraude interno</i> | 80 |
| Figura 10. <i>Simulación de categoría fraude interno</i> | 81 |
| Figura 11. <i>P-value para distribución de fraude externo</i> | 82 |
| Figura 12. <i>Distribución de datos de severidad ajustada a la distribución Lognormal para fraude externo</i> | 83 |
| Figura 13. <i>Simulación de categoría fraude externo</i> | 84 |
| Figura 14. <i>P-value para distribución Manejo y Ejecución de Procesos</i> | 85 |
| Figura 15. <i>Simulación de categoría manejo y ejecución de procesos</i> | 86 |
| Figura 16. <i>P-value para distribución fallas en el sistema e interrupción del negocio</i> | 87 |
| Figura 17. <i>Distribución de severidad ajustada a distribución Lognormal para fallas en el sistema e interrupción del negocio</i> | 88 |
| Figura 18. <i>Simulación de categoría fallas en sistemas e interrupción del negocio</i> | 89 |

Figura 19. *Simulación de pérdidas agregadas*.....90

Lista de Apéndices

| | Pág. |
|--|-------------|
| Apéndice A. <i>Probabilidades condicionales para fraude interno parte 1</i> | 101 |
| Apéndice B. <i>Probabilidades condicionales para fraude interno parte 2</i> | 101 |
| Apéndice C. <i>Probabilidades condicionales para fraude interno parte 3</i> | 102 |
| Apéndice D. <i>Probabilidades condicionales para fraude interno parte 4</i> | 102 |
| Apéndice E. <i>Probabilidades condicionales para fraude interno parte 5</i> | 102 |
| Apéndice F. <i>Probabilidades condicionales para fallas en sistema e interrupción del negocio</i> | 103 |
| Apéndice G. <i>Probabilidades condicionales para fraude externo</i> | 103 |
| Apéndice H. <i>Probabilidades condicionales para nodo calidad de personal</i> | 103 |
| Apéndice I. <i>Probabilidades condicionales para manejo y ejecución de procesos</i> | 104 |

Resumen

La presente investigación, tuvo como objetivo cuantificar el riesgo operativo en la línea de negocio de Banca Minorista de una sucursal bancaria en la ciudad de Bucaramanga, lo cual hizo posible conocer a detalle una metodología basada en enfoques ascendentes para estimar el riesgo operativo u operacional en entidades bancarias.

Para lo anterior, se definieron cuatro categorías de estudio de acuerdo al comité de Basilea para medir el riesgo operativo en la sucursal elegida, ellas fueron: Fraude Interno, Fraude Externo, Manejo y Ejecución de Procesos, y Fallas del Sistema e Interrupción del Negocio.

Los enfoques mencionados fueron: Redes Bayesianas que corresponden a la clasificación de modelo causal, y distribuciones de pérdidas que pertenecen a modelos estadísticos, las cuales fueron simuladas haciendo uso del método de Montecarlo.

Los datos requeridos para alimentar los modelos desarrollados fueron obtenidos mediante valoraciones cuantitativas en forma de probabilidades a priori y condicionales por parte de las creencias de especialistas en Riesgo Operativo en entidades bancarias, y por profesionales que han tenido experiencias y brindan sus servicios en sucursales bancarias tales como la analizada en la presente investigación, los resultados pueden observarse en el capítulo Análisis e Interpretación de Resultados.

Palabras claves: Banco, Bayesiana, Categoría, Montecarlo, Experto, Operativo, Red, Riesgo, SARO.

Abstract

The objective of this research was to quantify the operational risk in the Retail Banking business line of a bank branch in the city of Bucaramanga, which made it possible to know a detail of a methodology based on bottom-up approaches to estimate the operational or operational risk in Bank entities.

For the above, four study categories were defined according to the Basel committee to measure the operational risk in the chosen branch, they were: Internal Fraud, External Fraud, Management and Execution of Processes, and System Failures and Business Interruption.

The mentioned approaches were: Bayesian networks that correspond to the causal model classification, and loss distributions that belong to statistical models, which were simulated using the Monte Carlo method.

The data required to feed the developed models were obtained through quantitative valuations in the form of a priori and conditional probabilities by the beliefs of specialists in Operational Risk in banking entities, and by professionals who have had experiences and provide their services in bank branches. such as the one analyzed in the present investigation.

Keywords: Bank, Bayesian, Category, Montecarlo, Expert, Operative, Network, Risk, SARO.

Introducción

El RO (Riesgo Operativo), ha representado en los últimos años un desafío para la banca tanto internacional como nacional. El Comité de Basilea como organismo mundial de supervisión de los procesos y procedimientos del negocio bancario, ha dictado parámetros para establecer sistemas de gestión del riesgo que puedan controlar la exposición al mismo de actividades propias de las instituciones financieras que cada vez se hacen más complejas de entender [1].

Para analizar los factores que influyen sobre las posibilidades de que existan eventos de pérdidas al interior de cada sucursal bancaria, se requiere según expertos conocer los procesos que se generan y llevan a cabo en las diferentes líneas de negocio establecidas de forma estándar para la banca internacional.

Por la disponibilidad de la información para alimentar los modelos existentes para medir el RO en cualquier contexto, se hizo indispensable recurrir a expertos o especialistas y profesionales que han tenido, y tienen experiencia en la operatividad de dentro de la línea de negocio analizada, proporcionando valoraciones en términos de probabilidades a priori y condicionales, y de igual manera distribuciones de frecuencias y severidades para cada categoría sujeta al modelo estadístico desarrollado [2].

Para dar respuesta a los objetivos planteados, y pregunta problemática, se utilizaron como herramientas para el análisis de los datos y diseño de la Red Bayesiana de cada categoría software como Hugin Lite 8.9 y Risk Simulator.

1. Definición del Problema

1.1 Descripción del Problema

Todo país con un sistema financiero establecido bajo normas de regulación, y específicamente un sistema bancario, tiene a su disposición el principal mecanismo para movilizar recursos a los distintos sectores productivos que integran su economía. Por consiguiente, el protagonismo que recae en un sistema financiero es tal que, si se administra deficientemente no provoca solo la quiebra de ciertas entidades, sino que además genera la intervención por parte de entes gubernamentales, lo que, a final resulta en un desequilibrio para la economía en su conjunto, si no hay mecanismos eficientes y sofisticados de control. [3].

Así como las distintas empresas que no pertenecen al sector financiero, las que si hacen parte de este conglomerado, a lo largo de los últimos años han venido reflexionando sobre los riesgos e incertidumbre que enmarcan al mundo financiero de las distintas corporaciones, debido a que fallas presentadas en sus sistemas de tecnologías de la información e infraestructura tecnológica han significado importantes sumas económicas en pérdidas por errores en los diferentes procesos internos de las empresas. Lo anterior, sumado a eventos externos como fraudes e interrupciones de actividades operativas, hace parte de uno de los riesgos financieros causantes de los niveles más altos de pérdida para la banca, esto es el RO (Riesgo Operativo), el cual es inherente a las actividades diarias del negocio donde intervienen factores como: recurso humano, procesos, y sistemas de interconexión tecnológicamente complejos. [4]

Someramente, el RO corresponde a una pequeña porción de la totalidad de pérdidas anuales de las entidades financieras y bancarias; es así, que tales saldos negativos pueden provocar la liquidación de una empresa. Dada estas condiciones, una gestión eficaz que prevenga el RO, constituye un proceso de inmenso valor aplicativo para cualquier compañía, y es de mayor importancia que el medir la probabilidad de pérdida después de ocurrido el suceso [4].

Teniendo en cuenta que la administración de los procesos y sistemas de información se da por las personas desde sus respectivos cargos, la responsabilidad de incurrir en falla, cae sobre tal personal humano; esto, por realizar una acción que no debe de haber realizado, o por el contrario, al dejar de ejecutarla cuando en realidad si debía haberla llevado a cabo [4].

Actualmente ninguna entidad bancaria que se encuentre supervisada por la Superintendencia Financiera de Colombia, está exenta de caer en fallas de orden operacional, las cuales tarde o temprano se verán reflejadas en inconformidades por parte de los clientes ya sea a modo de molestias, solicitudes, y demás trámites correspondientes a quejas y reclamos. Este tipo de situaciones, aunque son seguidas en tema de calidad por los establecimientos bancarios, dejan ver que existen riesgos asociados a los procesos que requieren necesariamente ser controlados, de tal manera que en la situación más pesimista se materialicen a un mínimo, esto sin dejar a un lado, que traen consigo costos asociados a eventos de pérdida [5].

De acuerdo a la literatura referente al Riesgo Operativo, uno de los mayores obstáculos al momento de estimar cuantitativamente este tipo de riesgo financiero, es localizar una base de datos que contenga las variaciones del ambiente de trabajo de forma

completa, una clasificación de los diversos factores que conforman al RO, y establecer complejas interacciones entre las variables que lo caracterizan e identifican; es decir medir el RO, requiere de técnicas estadísticas dinámicas cuando los contextos no contienen fuentes de información tan claras [4].

Partiendo de lo traído a líneas respecto a la problemática descrita, en esta investigación se propuso construir un modelo causal basado en RB (Redes Bayesianas), que mediante la utilización de información inicial dada por expertos en los procesos internos de la entidad, se determinaran probabilidades a priori que permitieran cuantificar el Riesgo Operativo en una sucursal bancaria de la ciudad de Bucaramanga, actualizando los posibles eventos de pérdidas mediante las probabilidades a posteriori que representen probabilidades de pérdidas esperadas en un contexto futuro, tal proceso, buscó responder la siguiente pregunta:

1.2 Formulación del Problema

¿Qué variables de las que conforman el Riesgo Operacional son las que, a partir de una Red Bayesiana, generan los mayores niveles de probabilidad de pérdida en la línea de negocio analizada en una sucursal de bancaria en la ciudad de Bucaramanga?

1.3 Justificación

Dada la necesidad apremiante en el sistema bancario por brindar mayor seguridad a sus clientes e inversionistas en sus operaciones comerciales, han surgido distintas metodologías para cuantificar los diferentes riesgos financieros que pueden tener lugar en

tales actividades, y así mitigar al máximo los niveles de pérdida presentes en cada una de las líneas de negocio concernientes a la banca.

Para cualquier entidad bancaria, resulta de suma importancia controlar y monitorear los procesos que se llevan a cabo a su interior, sean estos coordinados por recurso humano o por sistemas inteligentes dotados de tecnología de punta.

El Comité de Basilea o Comité de Supervisión Bancaria de Basilea desde 1988, ha venido orientando a nivel mundial a los bancos estableciendo requerimientos mínimos de capital, así como una serie de prácticas internas de gestión que todas las entidades bancarias deberían de tener presente al momento de afrontar cualquier tipo de riesgo financiero. Exactamente en el año 2004, este comité de supervisión bancaria, ha establecido los cimientos mediante metodologías de análisis estadístico para un riesgo que antes era considerado no cuantificable, pero que a partir de entonces ha representado según el pensamiento del comité, peligros considerables para la solidez y seguridad del sistema bancario. De ahí, que lo que más interés ha generado en las entidades financieras como los son los bancos, es la adecuación de sus respectivos Sistemas integrales de Administración de Riesgos (SAR), a los parámetros establecidos por el Comité de Basilea, el cual, como principal objetivo tiene promover en las instituciones bancarias el cumplimiento de tres pilares fundamentales como lo son: el riesgo de crédito, el riesgo de mercado y el riesgo operativo [1].

A nivel internacional, son varios los modelos propuestos, reconocidos, y validados por la Superintendencia Financiera de Colombia, y es esto, lo que ha hecho reconocer, identificar e implementar, por parte de las entidades del sector financiero colombiano un

Sistema Integrado de Administración de Riesgo Operativo (SARO) que reduzca lo más posible el nivel de exposición a este tipo de riesgo [1].

Las circunstancias dadas históricamente, son las que han condicionado los distintos escenarios de análisis de Riesgo Operativo, donde son las aplicaciones estadísticas, en este caso Redes Bayesianas, las que permiten la cuantificación del RO dando valor probabilístico a las aproximaciones teóricas de los modelos que ya han sido realizados en distintos contextos.

Lo anterior, aportó una investigación aplicable a una sucursal bancaria en la ciudad de Bucaramanga, y sirvió como soporte para mejorar sus procesos de gestión de riesgo; teniendo en cuenta que las actividades que pertenecen a los mismos, están expuestas a errores humanos que ponen en riesgo al negocio financiero en cuanto al manejo y control de tales procedimientos operativos.

1.4 Alcance

Para la banca, lograr una estabilidad en el desarrollo de las operaciones comerciales que cada día se llevan a cabo en las distintas entidades del sector es primordial, por eso, es de gran interés para una institución de este ramo, tener el control de los procedimientos realizados, ya que tales actividades interrelacionadas comprometen activos importantes para las empresas involucradas.

La supervisión de todos los procesos, así como la cuantificación de los riesgos financieros a los que está expuesta una corporación dentro de la industria, en últimas se traduce en una manera de brindar confianza a los ahorradores e inversionistas de las compañías que conforman la industria de servicios financieros.

Gestionar de manera eficaz y eficiente los distintos tipos de riesgo financieros que se pueden presentar en una entidad bancaria, requiere de aplicar metodologías confiables, científicas, y seguras para evitar posibles pérdidas, ya sea de información o económicas en un mercado fuertemente influenciado por el factor tecnología. Es por ello, que, en el presente trabajo investigativo, se buscó cuantificar el Riesgo Operativo al que una sucursal bancaria de la ciudad de Bucaramanga puede estar expuesta, ya sea por “una insuficiencia o falla de los procesos, gente y sistemas internos o por acontecimientos externos” [2].

Para la consecución de los objetivos trazados, se utilizó un modelo causal implementando Redes Bayesianas propio del contexto estudiado. La metodología propuesta, se eligió debido a que, su aplicación como modelo, es útil cuando se carece de: datos históricos, confiabilidad en los datos o facilidad en la modelación de los mismos, en comparación con otras técnicas, ya que antes de ser considerados son validados por expertos con la finalidad de dar una parametrización a su posible comportamiento.

Todo lo anteriormente descrito, desde la escogencia del tipo de riesgo hasta la modelación de las variables que influyen en su probabilidad de ocurrencia dentro de la sucursal, facilitó construir una herramienta de gestión del Riesgo Operativo aplicable a la entidad bancaria seleccionada cuyo alcance se estuvo limitado exclusivamente al riesgo con la naturaleza estudiada en el proyecto.

2. Objetivos

2.1 Objetivo General

Construir una red bayesiana para medir el riesgo operativo en una sucursal Bancolombia de la ciudad de Bucaramanga.

2.2 Objetivos Específicos

- Evaluar los métodos existentes para la medición del riesgo operativo de entidades financieras por medio de la revisión de la literatura sobre el problema, basada en modelos causales.
- Construir un modelo causal empleando redes bayesianas para la medición del riesgo operativo de una entidad bancaria de la ciudad de Bucaramanga.
- Validar la red bayesiana utilizando el juicio de expertos, para verificar el cumplimiento de los parámetros asociados al modelo causal desarrollado.

3. Marco Referencial

3.1 Marco Teórico

3.1.1 *Redes Bayesianas*

Las RB (Redes Bayesianas), constituyen una herramienta de modelado estadístico orientada a la representación de un grupo de incertidumbres relacionadas. Este tipo de técnica con estructura y fundamentación probabilística, están dadas para plantear modelos de sistemas multivariados, cuyo fin es la clasificación, el diagnóstico y la toma de decisiones [6].

También puede entenderse una RB, como un grafo que cumple las siguientes características:

1. Nodos de la red conformados por un conjunto de variables aleatorias que se denotan con la letra X , o con subíndices X_1, X_2, \dots, X_n . Inicialmente tales variables pueden ser o representar rasgos, pero puede darse el caso que un mismo rasgo, requiera ser descompuesto en varias variables aleatorias. Ejemplo: si el rasgo dado es multivaluado y se desean las variables aleatorias dicotómicas [7].

2. Cada par de nodos se conecta entre sí mediante un conjunto de enlaces o de flechas. El significado de una flecha que vaya del nodo X al nodo Y , es el de que X , ejerce una influencia directa sobre Y ; en términos de probabilidades esto significa que hay una dependencia condicional de Y , con respecto a X , y que la probabilidad de Y , es diferente de la probabilidad de Y dado X [7].

3. Por cada nodo hay una tabla de probabilidad condicional que sirve para cuantificar los efectos de los padres sobre el nodo. Los padres de un nodo son aquellos nodos cuyas flechas apuntan hacia éste [7].

4. El grafo no tiene ciclos dirigidos (por lo tanto, es un grafo acíclico dirigido (GAD)). Esto significa, que no se presentan ambigüedades en el encadenamiento de probabilidades condicionales por el hecho de tener influencias directas cíclicas [7].

Al hacer una referencia directa a las redes bayesianas, necesariamente tocaría hablar de su fundamento teórico, el cual toma base científica en el teorema de *Thomas Bayes* (1702-1761).

Dentro de la teoría probabilística el teorema de *Bayes*, también conocido como el teorema de las causas, está dado por:

$$P(A|B) = P(B \cap A) / P(A) \text{ Tomado de: [8]}$$

En términos generales, la importancia de este teorema radica en que vincula la probabilidad de A dado B , con la probabilidad de B dado A [8].

La probabilidad a priori de un evento futuro incierto y la probabilidad condicional de los resultados de la muestra deben ser conocidas, estas últimas están determinadas por la aplicación de una norma de distribución de probabilidad acorde a al carácter de tal distribución [8].

3.1.2 Conceptos para la Comprensión del Teorema de Bayes

3.1.2.1 Sucesos o Eventos. Subconjuntos del espacio muestral Ω asociados a un experimento ϵ [8].

3.1.2.2 Sucesos Mutuamente Excluyentes. Dados dos sucesos A y B, se dice que ambos son mutuamente excluyentes, sino pueden tener lugar su ocurrencia de manera simultánea, lo anterior se denota: $A \cap B = \emptyset$ [8].

1. si el evento A es nulo, $A = \emptyset$, se tiene que $P(A) = P(\emptyset) = 0$ [8]

2. sean $\{A_1, A_2, \dots, A_n\}$ sucesos mutuamente excluyentes ($A_i \cap A_j = \emptyset$ si $i \neq j$) por lo que se tiene que: $P(\bigcup_{i=1}^n A_i) = \sum_{i=1}^n P(A_i)$ [8].

3. sean A y A^c eventos complementarios, $A \cup A^c = \Omega$, es decir la unión de dos eventos complementarios es la equivalencia con el espacio muestral, se tiene que $P(A) + P(A^c) = 1$ para todo evento A en Ω [8].

4. sea $(A \cup B)$, el evento definido como que ocurra A u ocurre B, se tiene que $P(A \cup B) = P(A) + P(B) - P(A \cap B)$ [8].

3.1.2.3 Probabilidad Condicional. Es un tipo de probabilidad que permite modificar la creencia que se tiene acerca de la realización de un experimento aleatorio [8].

Dado un evento B, la probabilidad condicional de que un suceso A ocurra, queda definida de la siguiente manera:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \text{ Tomado de: [9]}$$

Lo anterior siempre que $P(B) > 0$. [El símbolo $P(A|B)$ se interpreta como “probabilidad de A dada B”]

3.1.3 Fundamentación de las Redes Bayesianas

El surgimiento de las Redes Bayesianas, se da por la necesidad de mejorar de manera sustancial en términos de calidad el proceso de clasificación de datos, con el propósito de no caer en suposiciones sobre los diversos atributos que pueda tener una información. Este tipo de técnica estadística busca posibilitar de forma práctica la representación eficiente y el razonamiento riguroso con conocimiento incierto [10].

Una de las características más importantes de las Redes Bayesianas, es que permiten aprender a realizar un aprendizaje partiendo de relaciones de dependencia y causalidad, combinando ambas conocimiento con datos [11].

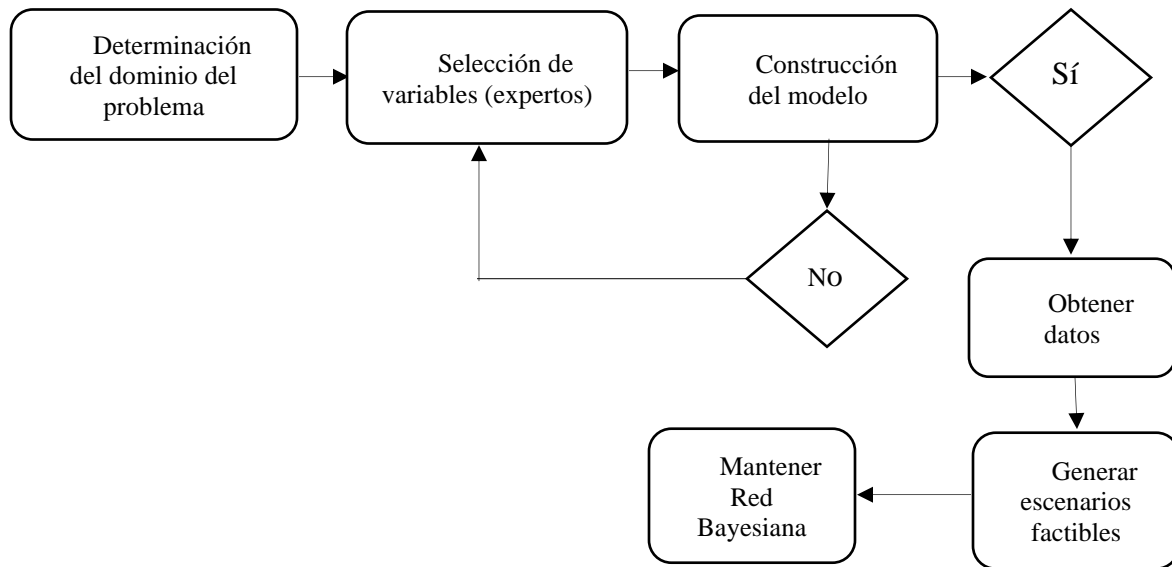
Ya que brinda la facilidad de entenderla, una red bayesiana, permite realizar una extracción de lo que pueden llegar a ser las explicaciones con más probabilidad de ocurrencia dentro de una determinada observación, en la que se considera también el conocimiento de manera cualitativa. Atendiendo a la descripción anterior, características de la información como variabilidad e incertidumbre dadas en algún proceso, pueden ser tratadas de forma probabilística por medio de redes bayesianas, incorporando distribuciones de probabilidad para distintos intervalos de tiempo teniendo previamente determinadas unas condiciones iniciales [8].

Cabe resaltar que el realizar inferencia bayesiana en la elaboración de una red, radica su aplicabilidad en extraer información obtenida por las variables que son manipuladas en el proceso de construcción de la RB, después de ser compradas con las variables que no son observadas. Ello hace factible describir posibles relaciones entre las variables partiendo de los datos [12].

Una gran aplicación que se consigue utilizando las Redes Bayesianas, es el poder hacer más eficaz el proceso de toma de decisión en una organización. Esto se logra mejorando las estimaciones de probabilidad, para lo cual se requiere del teorema de Bayes para realizar estadísticas que permitan analizar los datos, lo cual facilitará al investigador hacer inferencias, realizar exclusiones u opiniones personales acerca del tema objeto de estudio [13].

El análisis estadístico bayesiano, se realiza para evaluar las acciones de la alternativa de decisión enmarcadas en un contexto con consecuencias económicas. Estas consecuencias económicas, se pueden formular como valores económicos o pérdida de oportunidad comercial dentro de un escenario evaluativo. Esta es una de las razones por la que la inferencia bayesiana viene a ser una alternativa de gran valor gerencial en el sector empresarial, la cual considera costos reales y oportunidades en que la mayoría de las veces deben realizarse en condiciones de incertidumbre [8].

Los casos basados en Redes Bayesianas, tienen en cuenta información histórica de los datos que corresponden a acontecimientos de riesgos, una forma es a través de indicadores de pérdida lo que permitirá explicar tal información en términos de finanzas. En este sentido, las Redes Bayesianas son construidas para señalar aquellos factores de riesgo operacional, representar la definición de una variable y la estimación de probabilidades de las distintas categorías de un evento; por lo que, al momento de su elaboración, los componentes a revisar son: probabilidades condicionales de la información histórica requerida al inicio, y la metodología de distribución de probabilidad según el caso de estudio considerado [8].

Figura 1. *Flujograma para construir una Red Bayesiana*

Adaptado de: Revista Contaduría y Administración -UNAM [14]

De acuerdo al flujograma para la construcción de una RB, cabe destacar que se hizo necesario determinar el dominio del problema a tratar, es decir, conocer el estado en el que se podría aplicar la metodología de Redes Bayesianas a la sucursal bancaria objeto de estudio. Un paso importante en la construcción del grafo o grafos, fue la identificación de los perfiles de los especialistas en el tema, los cuales fueron los encargados de diagnosticar en primera instancia como se encontraba el panorama a comprender, y a su vez, proporcionaron probabilidades subjetivas de cada posible evento de pérdida.

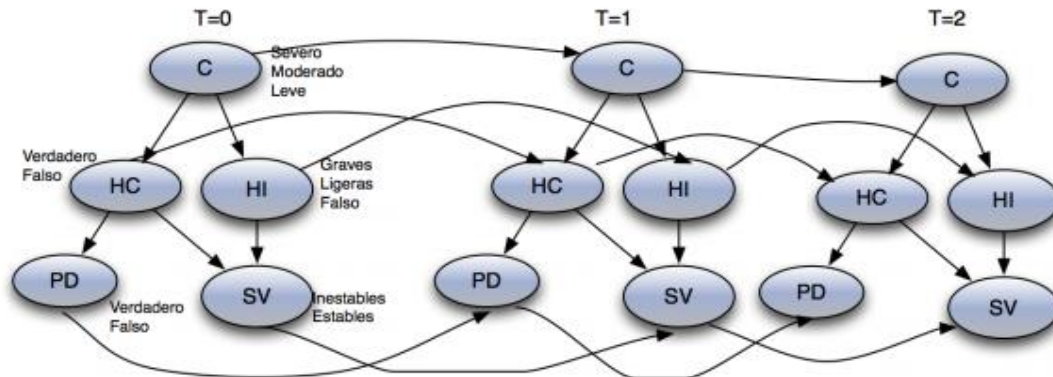
La guía recibida desde el flujograma de igual manera permitió diseñar el modelo en el tiempo oportuno, para luego ser alimentado por los datos dados por los expertos. Por último, se generaron los espacios factibles que luego fueron indicados para que para posibles estudios posteriores se puedan mantener las Redes Bayesianas construidas.

3.1.4 Tipos de Redes Bayesianas

3.1.4.1 Redes Bayesianas Continuas. Son aquellas redes que tienen un número infinito de posibles valores. Para este tipo de redes, resulta difícil determinar explícitamente las probabilidades condicionadas para cada valor de las variables, por lo tanto, las probabilidades condicionadas son representadas por una función de probabilidad. Una Red Bayesiana, cuyas variables sean todas continuas y estén todas representadas mediante funciones normales lineales, tiene una distribución normal multivariada. Por lo tanto, este tipo de variables debe ser tratado mediante el proceso de discretización, esto se debe al gran volumen de datos que deben ser modelados por medio de la selección de rango, lo cual hace más sencillo el proceso en mención [14].

3.1.4.2 Redes Bayesianas Dinámicas. Las Redes Bayesianas dinámicas, son aquellas que modelan la evolución estocástica de un conjunto de variables $X = \{X_1, \dots, X_n\}$ en el tiempo. En este tipo de redes bayesianas se consideran dos suposiciones: *los procesos son markovianos*; esto significa que las variables del periodo de tiempo actual son condicionalmente independientes de las variables de periodos anteriores. *Los procesos son estacionarios*; las probabilidades de transición entre un periodo y otro son independientes del tiempo [15].

En la Figura 2, se puede observar el grafo representativo de una Red Bayesiana Dinámica. Es decir, un grafo en el que las condiciones de los estados de naturaleza de cada nodo se comportan de forma distinta en los periodos anteriores, esto significa que las probabilidades de cada variable son independientes en cada estado del tiempo.

Figura 2. Red Bayesiana Dinámica. Representación de una Red Bayesiana Dinámica

Adaptado de: Repositorio institucional de INAOE [16]

3.1.5 Inferencia Bayesiana

En RB (Redes Bayesianas), el hablar de inferencia bayesiana consiste en: dadas ciertas variables que son conocidas (Evidencias), pueden calcularse las probabilidades posteriores de las demás variables (Desconocidas). Lo mismo en notación de probabilidad es: $P(X_i | E)$, donde E, representa un subconjunto de variables de la RB (posiblemente vacío).

Por otra parte, X_i , es cualquier variable en la RB, no en E [17].

Existen varios tipos de algoritmos para realizar el cálculo de las probabilidades a posteriori, y estos dependen tanto del tipo de grafo como si se obtiene la probabilidad de una sola variable o de todas. Los principales tipos de algoritmos para realizar inferencia bayesiana son:

3.1.5.1 Una Variable, Cualquier Estructura: Algoritmo de Eliminación. El algoritmo de eliminación de variables, consiste en un algoritmo en el que es posible obtener conocimiento a partir de una Red Bayesiana. Dada la RB, y un conjunto de valores para cada variable conocida (evidencia), se hace posible la estimación de probabilidades esperadas a partir de una o varias variables de consulta. En este orden, el algoritmo de eliminación de variables, utiliza diferentes técnicas para reducir cálculos de probabilidad desechando de tales cálculos, las variables que no guardan ninguna relación de dependencia con las ya existentes [18].

Esquema general de la eliminación de variables

- Construir matrices multidimensionales llamadas factores
- Factores iniciales: construir tablas de probabilidad condicional una por nodo.
- Seleccionar valores conocidos.
- Ir alternando, es decir unir factores y eliminar variables.

Considerando el ítem anterior, la operación de unir factores se realiza de la siguiente manera:

- Seleccionar factores parecidos en una base de datos.
- Tomar todos los factores que mencionan la variable a unir.
- Construir un nuevo factor con la unión de todas las variables involucradas.

En cuanto a la operación de la eliminación de variables en la estructura general, la misma sigue la forma siguiente:

- Marginalización: La marginalización en el presente algoritmo, corresponde a la concepción de eliminar nodos en el grafo construido. De acuerdo a un orden de las variables, se van eliminando nodos, conectando sus vecinos. [19]

- Tomar un factor, y sumar sobre una variable para quitarla; el factor se reduce de tamaño, dándose de tal manera una operación de proyección. [19]

Evidencia: en caso de haber evidencia, iniciar el algoritmo con los casos que la tomen.

3.1.5.2 Cualquier Variable, Estructuras Sencillamente Conectadas: Algoritmo de Propagación de Pearl. La idea del algoritmo de propagación de Pearl, consiste en que cuando la información asociada a un nodo se modifica, este traspasa la información a sus nodos vecinos mediante un conjunto de mensajes; estos nodos, a su vez, procesan la información recibida junto con las que ellos poseen y las pasan a sus nodos vecinos (aun no modificados) y así sucesivamente hasta que todos los nodos han actualizado la información que cada uno presenta [20].

El algoritmo principalmente consta de dos fases:

1. *Fase de inicialización.* En esta fase, se pretende obtener las probabilidades a priori de todos los nodos de la red, obteniendo un estado inicial de la red que puede notarse como S_0 [20].

2. *Fase de actualización.* En esta fase, se obtienen las probabilidades a posteriori de las variables de la red basadas en la evidencia considerada, adoptando la red un estado que puede denotarse como S_1 [20]. Este paso se repite cada vez que una variable se instancia, obteniéndose los sucesivos estados de la red.

Previamente cabe aclararse que, si existe un arco que enlaza a un nodo A con un nodo B, A es suele denominarse un padre de B, y B es considerado como un hijo de A [20].

La idea central que sigue este algoritmo es la siguiente:

Cada vez que una variable se instancia, la misma informa a sus nodos vecinos mediante el paso de lo que suele llamarse *mensaje*. Lo anterior se lleva a cabo de la siguiente manera:

- La variable envía a su padre un mensaje, denominado λ -mensaje, para informar del cambio de valor [20].
- La variable envía a todos sus hijos un mensaje, denominado π -mensaje, para informar del cambio de valor [20].

Es así como la información se va propagando por la RB, tanto en sentido ascendente como descendente.

Los mensajes dados entre cada par de nodos, asignan a cada variable unos valores λ -valor y π valor. Multiplicando tales valores, es posible obtener las probabilidades a posteriori de cada una de las variables de la red.

Figura 3. Ejemplo de estructura de una Red Bayesiana

Por ejemplo:



Adaptado de: [20]

Los valores como mensajes en las RB, son vectores de números; para el caso del arco presentando en el que la variable A presenta tres posibles valores a_1 , a_2 , y a_3 , y la variable B es binaria con valores b_1 y b_2 , se tendría que:

- Si se instancia la variable A, la misma enviaría un π -mensaje a B, $\pi_B(A)=(\pi_B(a_1), \pi_B(a_2), \pi_B(a_3))$.

- Si se instancia la variable B, esta enviaría un λ -mensaje a A, $\lambda_B(A)=(\lambda_B(a_1), \lambda_B(a_2), \lambda_B(a_3))$.

En función de los mensajes generados, se obtiene un λ -valor y una π -valor para A.

$$\lambda(A)=(\lambda(a_1), \lambda(a_2), \lambda(a_3)) \text{ y } \pi(A)=(\pi(a_1), \pi(a_2), \pi(a_3))$$

Así mismo, se obtiene un λ -valor y una π -valor para B.

$$\lambda(B)=(\lambda(b_1), \lambda(b_2)) \text{ y } \pi(B)=(\pi(b_1), \pi(b_2))$$

3.1.5.3 Cualquier Variable, Cualquier Estructura: Algoritmo de Agrupamiento

Según la literatura consultada, el algoritmo más común en Redes Bayesianas es el de agrupamiento o árbol de uniones (*junction tree*). El método de agrupamiento consiste en transformar la estructura de la red para obtener un árbol, mediante agrupación de nodos usando la teoría de grafos [21]. Para ello, se hace una transformación de la red a un árbol de uniones (grupos de nodos) a través del siguiente procedimiento:

- Eliminar la direccionalidad de los arcos.
- Ordenar los nodos por máxima cardinalidad (máximo número de asociaciones).
- Moralizar el arco (arco entre nodos con hijos comunes).
- Triangular el grafo.
- Obtener los cliques (subconjuntos de nodos completamente conectados máximo, de forma que hay un arco entre cada par de nodos) y ordenar.
- Construir árbol de cliques.

3.1.6 Simulación Estocástica

La simulación estocástica, es un método aproximado para la propagación de la evidencia en la RB, aplicable a cualquier estructura de red. En este método, se obtienen las probabilidades a posteriori de cada variable de forma aproximada. Lo que básicamente sucede en la aplicación del algoritmo, es que se generan muestras de tamaño N (número de nodos o tamaño de la red) a partir de las cuales se aproximan los valores de probabilidades buscados, considerando la frecuencia en la que aparece cada valor dado en la muestra, así como el tamaño de la misma [21].

Al final de la simulación, los pesos determinados son normalizados y utilizados en la estimación de las probabilidades a posteriori.

Para este algoritmo, se parte de la suposición de que existe un conjunto de variables $X = (X_1, \dots, X_N)$, con una función de probabilidad conjunto $P(x)$ y un subconjunto E de variables de X , que toma valores conocidos. Al darse una función de probabilidad conjunta $P(x)$, asociada a una RB, este método puede definir un modo específico de generar muestras y calcular sus pesos [21].

3.1.7 Algoritmo de Condicionamiento

Al instanciar una determinada variable de la RB, ésta bloquea las trayectorias de propagación, lo cual implica que si se asumen valores para un grupo seleccionado de variables; el condicionamiento permite la propagación de la evidencia para cada valor posible de tales variables, y posteriormente promediar las probabilidades ponderadas [21].

3.2 Marco Conceptual

1. *Arco*. “Subconjunto de pares ordenados” [22]

2. *Énfasis Bayesiano*. Aplicabilidad de la estadística bayesiana a través de técnicas estadísticas que permiten simular y explicar contextos enmarcados por factores de incertidumbre [22].

3. *Fallo*. Atributo que permite conocer que factores inciden en la probabilidad de incurrir en un fallo ya sea de un proceso, maquina o procedimiento [22].

4. *Fallo Humano*. Atributo que está asociado a la responsabilidad de quienes intervienen en los procesos, maquinaria o procedimientos, causan fallas operativas dentro del sistema [22].

5. *Grafo*. “Par de conjuntos $G = (X, L)$, donde X es un conjunto finito de elementos (nodos), y L un conjunto de arcos” [22].

6. *Grafo A cíclico*. “Grafo que no tiene ciclos” [22].

7. *Grafo dirigido*. “par ordenado $G = (X, L)$, donde X es el conjunto de nodos y L es el conjunto de arcos” [22].

8. *Riesgo Financiero*. “Probabilidad de que suceda un evento con consecuencias financieras negativas para una organización” [23].

9. *Entidad Bancaria*. “Institución financiera de intermediación que recibe fondos en forma de depósito de las personas que poseen excedentes de liquidez, utilizándolos posteriormente para operaciones de préstamos a personas con necesidad de financiación, o para inversiones propias” [24].

10. *Entidad Financiera*. “Es cualquier entidad que ofrece servicios financieros, sea cual sea su modalidad, a su clientela. Son aquellas que operan en el sistema financiero en

cualquiera de las tres grandes áreas en las que estos se dividen: Banca, Valores y Seguros” [25].

11.*Riesgo Legal*. “Consiste en la posibilidad a la que una organización puede incurrir en pérdida al ser sancionada o indemnizar daños como consecuencia por incumplimiento de normas, regulaciones y obligaciones contractuales” [1].

12.*Riesgo Reputacional*. “Tipo de riesgo al que una entidad puede caer por desprestigio, mala imagen, publicidad negativa, teniendo como consecuencia la pérdida económica y pérdida de clientes” [1].

13.*Riesgo Inherente*. “Consiste en el nivel de riesgo propio de la actividad que se esté realizando, sin tener en cuenta los efectos de los controles” [1].

14.*Riesgo de Crédito*. El riesgo de crédito es el tipo de riesgo relacionado a la incapacidad o no intencionalidad de una contraparte para darle cumplimiento a las obligaciones de una emisión o con los términos contractuales de la misma, entre los factores que la conforman estas: el capital, intereses y plazos, causando pérdida a quien es propietario de los activos [1].

15.*Riesgo de Mercado*. El riesgo de mercado, es un tipo de riesgo que guarda relación con la variabilidad en los resultados financieros de una organización, originados por variables del mercado donde participa, entre las variables que se destacan se encuentran: el precio, tasa de interés, tasa de cambio, inflación, etc. [1].

16.*Riesgo Estratégico*. “Riesgo asociado a la incertidumbre en los resultados financieros debido a decisiones estratégicas tomadas por la empresa, las cuales pueden tener repercusiones directas en el posicionamiento y reputación de la entidad en el escenario donde comercialmente participa” [1].

3.3 Marco Histórico

Históricamente el riesgo operativo cobra significado para la banca mundial desde años atrás cuando en 1974 inicialmente los gobernadores de los principales bancos centrales del G10, empezaron a unificar criterios sobre la supervisión y control de las operaciones que se llevaban a cabo en las respectivas entidades del sector [26].

Tales concurrencias en sus diversas opiniones y pensamientos de cómo deberían realizarse las actividades operacionales de los bancos, dieron origen a lo que actualmente se conoce con el nombre del Comité de Supervisión Bancaria de Basilea, que, aunque no tener una naturaleza supranacional, si buscaba mediante la formulación de estándares de supervisión para el sector bancario fortalecer la estabilidad monetaria y financiera mundial [26].

A partir del momento anteriormente descrito, en 1975 el comité emite una serie de documentos guías para buenas prácticas operativas que posteriormente han tenido que ser perfeccionadas. En 1999, los países no pertenecientes al G10, empiezan a desarrollar una relación estrecha que a través de una metodología de principios básicos de supervisión bancaria, el comité de Basilea facilitaría para su respectiva aplicación y evaluación en los países socios de sus métodos de control y estabilidad financiero [26].

Cuando se originó el mundo corporativo, la posibilidad de sufrir cualquier fraude ha estado presente, ya sea de forma interna o externa. La eventualidad de que un sistema falle operacionalmente fue lo que, hasta hace algunos años, dio lugar al estudio del riesgo operativo en instituciones financieras, quienes por consecuencias asociadas a este tipo de riesgo han llegado a condiciones de quiebra. De ahí que tanto entidades como los entes reguladores, reconocen desde las experiencias vividas, que la necesidad para el sistema

financiero radica en conocerlo a profundidad y establecer herramientas que permitan su cuantificación [27].

Revisando dicha acontecimientos dados en el ámbito financiero internacional, y considerando las pautas de control y supervisión para las operaciones bancarias establecidas por el Comité de Basilea, desde el 2006 la Superintendencia Financiera de Colombia(SFC),a través de la circular externa 048 del 22 de diciembre de 2006,dicto para todas las entidades bajo su supervisión,las bases y los lineamientos mínimos para el desarrollo de un Sistema de Administración de Riesgo Operativo(SARO),que desde dicha data, ha representado la obligación para las entidades bancarias de enfrentar retos como la globalización de la oferta de servicios financieros, la modernización de la tecnología utilizada en sus plataformas y la diversificación de nuevos productos en los últimos años [28].

En la Tabla 1, se establecieron aquellas normas que según la reglamentación vigente para controlar operativamente las actividades del sector financiero existen.

Dentro de las normas que se encontraron se encuentran documentos correspondientes a circulares, en los que se parametrizan los aspectos a tener en cuenta en el control y la supervisión de aquellos factores que inciden de gran manera en la exposición al riesgo que una sucursal bancaria podría llegar a percibir.

Otro detalle importante de las circulares encontradas es que, la existencia de un Sistema de Administración del Riesgo Operativo (SARO), se ve reflejado en las pautas a seguir por partes de las instituciones financieras en Colombia recomendadas y sugeridas por el Comité de Basilea, organismo internacional de supervisión de las actividades bancarias.

Para tales recomendaciones caben aclarar que, son implementaciones que se han acogido en la banca nacional no tan antiguamente.

3.4 Marco Normativo

Tabla 1. Normas

| Norma | Objeto | Aporte de la Norma a la investigación |
|-------------------------------------|---|---|
| Circular externa 048 de 2006 | Instrucciones relativas a la adopción de un Sistema de Administración de Riesgo Operativo (SARO) [29] | Este documento con contenido técnico y de gestión busca impulsar en materia de administración y control de riesgo operativo las bases y lineamientos mínimos para el caso colombiano de la adopción adecuada de un SARO. Tal circular permite conocer: 1.La importancia de contar con una adecuada administración de riesgo operativo. 2.Aunque este riesgo no considerado generalmente financiero, no difiere en sus componentes ni elementos de uno que propiamente si lo es. 3.Coloca al mismo nivel de importancia la administración del riesgo operativo con la de los riesgos de crédito, mercado, liquidez, y demás. [29] |
| Circular externa 041 de 2007 | Las entidades deben diseñar, programar y coordinar planes de capacitación anuales sobre Riesgo Operacional (RO) para sus empleados y para los terceros con quienes existe una relación contractual y desempeñan funciones de la entidad. [30] | La importancia de esta circular para el proyecto subsiste en que permite someramente conocer un esquema de capacitaciones que a través de Asobancaria se pretende capacitar a los actores del sector financiero en la identificación, medición y reporte de los riesgos operacionales presentes en los servicios y procesos que prestan los bancos del país. [30] |

Nota: * Normas aplicadas al manejo del Riesgo Operativo en entidades financieras. Adaptado de: Asobancaria, Superintendencia Financiera de Colombia.

3.5 Estado del Arte

La importancia que ha tenido actualmente el Riesgo Operativo en el sector bancario, está dada, por la cantidad de factores interrelacionados en las operaciones financieras que las hacen susceptibles de caer en fallas humanas, lo que al final puede traducirse en pérdidas para cualquier organización financiera; esto, porque se llevan a cabo “procesos internos inadecuados o defectuosos, fallas en los sistemas, y errores inducidos por acontecimientos externos” [31].

No es una situación fácil de eludir dentro del contexto financiero, el eliminar o reducir al máximo la existencia del Riesgo Operativo, debido a que se trata de un “tipo de riesgo inherente a todas las actividades, productos, sistemas, y procesos con orígenes y causas variadas como lo son: procesos, fraudes internos y externos, tecnologías, recursos humanos, prácticas comerciales, desastres, proveedores” [31].

Han sido los distintos eventos de crisis financieras últimamente ocurridos en la economía mundial, los que han propiciado la necesidad de crear metodologías para medir o cuantificar los distintos riesgos a los que pueden estar las entidades financieras en exposición.

Este aparte tiene como propósito, sistematizar de forma coherente la literatura concerniente a la cuantificación del riesgo operativo en una entidad financiera, métodos y modelos utilizados para ello, revisando específicamente el uso de Redes Bayesianas para tal fin.

Citando a [32], quienes en su artículo titulado: “*Riesgo Operacional en la Banca Transnacional*”, expresan que la calibración de los modelos de Red Bayesiana, debe incluir fuentes de información tanto objetivas como subjetivas, esto para lograr establecer de manera adecuada, la correcta interrelación causa-efecto, que pueda llegar a existir en los factores de

riesgo que intervienen en el análisis del tipo operacional. De acuerdo a lo propuesto por los autores, la cuantificación del RO, requiere que los parámetros tenidos en cuenta en la construcción de las redes sean considerados como variables aleatorias que sigue una determinada distribución, siendo tal distribución de naturaleza a priori, independiente de los datos de estudio y dependiente de la información y conocimiento respectivo que los expertos tengan del tema estudiado.

Para alcanzar los objetivos propuestos [32], determinaron y analizaron estadísticamente una red de frecuencia y una red de severidad para cuantificar las probabilidades de ocurrencia de los posibles eventos de pérdidas, que posteriormente sirvieron para el cálculo de las probabilidades a posteriori, utilizando técnicas de inferencia bayesianas como el algoritmo *Junction tree*. En este trabajo, por el solo error humano para el caso estudiado las probabilidades de pérdidas ascendieron a 152 millones de euros mensuales y para lo que respecta a fallas de sistemas, en promedio se encontró una pérdida de 318 millones de euros mensuales.

En el artículo “*Modelling Operational Losses: A Bayesian Approach*”, [33] afirman que uno de los problemas a la hora de cuantificar el Riesgo Operacional, es la escasez de datos de pérdidas. Los investigadores, utilizaron una metodología para resolver este punto crítico a través del teorema de Bayes. La Red bayesiana construida para el contexto analizado, permitió la integración coherente de diferentes fuentes de información como datos internos y externos, opiniones de expertos (propietarios de procesos) sobre la gravedad y frecuencia de cada evento de pérdida.

En “*Cálculo del Valor en Riesgo Operacional de una Empresa Aseguradora Mediante Redes Bayesianas*”, [34], dan a conocer otra aplicación de las RB en la

cuantificación del Riesgo Operacional en instituciones financieras. Como propósito de investigación plantean, el desarrollo de una metodología fundamentada en Redes Bayesianas con aras de identificar y estimar cuantitativamente el Riesgo Operacional que debe ser considerado para determinar el capital de solvencia durante el proceso de cotización de pólizas en la línea de una entidad aseguradora.

El modelo construido en este trabajo investigativo que considera probabilidades tanto a priori como a posteriori, permitió cuantificar la frecuencia y establecer la severidad de los posibles eventos de perdidas, y para las a posteriori la cuantificación de las pérdidas estimadas a un año, se hizo mediante la simulación de Montecarlo.

Para la construcción del modelo propuesto, se identificó las áreas de operación de la aseguradora que realmente son dos las más importantes: suscripción del riesgo e inversiones de capital. Seguidamente el proceso de construcción fue dividido en 2 fases: construcción del modelo y cuantificación de la red; la construcción del modelo, que en breves palabras es la definición del dominio de la red, que para el caso estudiado fue la línea de cotización. Luego tuvo lugar en la metodología la identificación de las variables o nodo importantes, los cuales consecutivamente fueron interrelacionados para la elaboración de los grafos. Representadas las interrelaciones en las Redes Bayesianas, el modelo fue puesto a consideración de expertos quienes buscaron mediante consensos llegar a un acuerdo sobre la calibración y cuantificación para ponerla en marcha en escenarios factibles.

[35] en “*Modeling Operational Risk With Bayesian Network*”, exponen que las Redes Bayesianas, han sido utilizadas como una herramienta que permite llevar a cabo una supervisión de las instituciones financieras, especialmente bancos y compañías de seguros, ofreciendo un modelado del Riesgo Operativo. Los autores del trabajo mencionado, afirman

que generalmente para cuantificar el Riesgo Operacional, se utilizan modelos lineales como: series de tiempo, modelos econométricos, modelos actuariales empíricos, y teoría de valores extremos. Pero debido a las limitaciones de los datos al momento de implementar uno de los modelos anteriores, así como las complejas interacciones entre variables existentes, han surgido modelos no líneas como lo son las Redes Bayesianas que permiten modelar varios factores de riesgo, y combinarlos en una distribución general de pérdidas.

Los investigadores sostienen en su trabajo investigativo, que al aplicar la metodología de Redes Bayesiana es posible: (1) formar distribuciones marginales posteriores de variables basadas en evidencias, (2) simular escenarios, (3) actualizar los parámetros del modelo utilizando datos, y (4) cuantificar en tiempo real qué tan bien se comparan las predicciones del modelo con los datos reales.

Dándole continuidad al Riesgo Operacional desde un enfoque Bayesiano, y resaltando los hallazgos identificados en la recopilación sistemática de información con relación a la cuantificación de este riesgo financiero, y desde la posición de [36], se reafirma lo expuesto en los trabajos citados anteriormente, expresando que a la hora de identificar y cuantificar el Riesgo Operativo mediante una RB, se debe calibrar el modelo utilizando fuentes objetivas y subjetivas, para un tratado correcto de la interrelación existente entre los diferentes factores que lo componen. En el artículo: “*Riesgo Operacional en el Proceso de Pago del Procampo, Un enfoque Bayesiano*”, se plantea una experiencia aplicada al proceso de pago del Programa de Apoyos Directivos al Campo (PROCAMPO), México, durante el periodo 2008-2011. Para este caso en condiciones de incertidumbre, la información utilizada inicialmente para la distribución de probabilidad a priori se llevó a cabo incluyendo

información subjetiva en la toma de decisiones, la opinión de expertos y juicios de analistas, de los eventos del proceso de bancarización.

Para el cálculo de las probabilidades a posteriori, se sigue dando la aplicabilidad del algoritmo *Junction Tree*, y para la cuantificación del RO condicional, se utilizó la simulación de Monte Carlo con las distribuciones a posteriori encontradas para las redes de severidad y de frecuencia. Finalmente, se compararon los resultados dados con redes bayesianas y otros con métodos clásicos, y se expusieron los resultados y conclusiones que se tuvieron como derivados del trabajo.

Así mismo, [37] en *“Operational Risk Measured by Bayesian Networks with a Poisson-Gamma Joint Distribution in a Financial Firm”* sus autores buscaron cuantificar los requerimientos de capital y Riesgo Operacional a través de inferencia Bayesiana, mediante un modelo de distribución conjunta Poisson-Gamma alimentado por información de expertos para una institución financiera mexicana. En esta investigación, simulaciones de Monte Carlo basadas en intervalos del valor esperado del evento de pérdida mostraron que: (1) el valor del riesgo operacional puede ser calculado con información insuficiente con 95% de confianza, (2) las pérdidas esperadas tienden a incrementar cuando los sucesos que esperan los expertos, también se aumentan, (3) hay una correlación positiva entre el riesgo operacional y los eventos esperados por los expertos, (4) la frecuencia y severidad de las pérdidas son más pequeñas al principio y luego crecen conforme el valor en riesgo operacional se acerca al óptimo, después ambos tienden a disminuir nuevamente.

Ubicando la aplicación Bayesiana a la estimación del RO para entidades del sector financiero Colombiano, se ha encontrado que dentro de las experiencias halladas, se destaca *“Modelo de Gestión para Riesgo Operativo aplicado al proceso de Fábrica de Crédito en la*

Cooperativa Originar Soluciones “planteada por: [38], donde la metodología sigue las pautas ya mencionadas anteriormente, y dentro de las principales conclusiones obtenidas están: las Redes Bayesianas, son un una opción para cuantificar las pérdidas esperadas en una compañía ya que son consistentes, aun cuando haya lugar a la falta de información histórica y registros de eventos.

De igual manera se afirma como conclusión, que un proceso de Gestión y administración del RO, es de vital importancia ya que, para el caso estudiado, al interior de la cooperativa permitió identificar el impacto que hay en la línea analizada, realizando de forma adecuada la modelación parametrizada propuesta con base a indicadores de riesgo.

Así mismo se ha encontrado un estudio de [39]” *A Bayesian Networks approach to Operational Risk*”, en el que las pérdidas internas obtenidas para un banco objeto de estudio, se promediaron sobre un horizonte temporal variable, de manera que las correlaciones encontradas entre los distintos procesos internos fueron eliminadas en algunos momentos, mientras se mantuvieron tales correlaciones al mismo tiempo para ciertas circunstancias. Estos promedios, son adecuados según los autores, para determinar los parámetros de la red. El algoritmo, fue validado en series temporales sintéticas.

La importancia de implementar Redes Bayesianas en la cuantificación del Riesgo Operativo de una entidad financiera, se ve reafirmada en el estudio de [40], quien en *“Bayesian Methods for Measuring Operational Risk”*, deja en manifiesto que las Redes de Creencias Bayesianas (BBN) y los diagramas de influencia sirven para medir y gestionar ciertos riesgos operativos, como los riesgos de procesamiento de transacciones y riesgos humanos. De acuerdo al autor, las BBN se prestan al modelado causal de procesos operativos,

siempre y cuando se puedan identificar los factores causales; dado esto, la Red Bayesiana modelará las influencias entre estos factores y su contribución al desempeño del proceso.

La aplicación de la metodología en cuanto a tiempo, depende del propósito del investigador y del alcance de la investigación, un caso en el que se toma un límite de tiempo para llevar a cabo una investigación de este tipo es:” *An analysis on operational risk in international banking: A Bayesian approach (2007-2011)*”, en la que [41] desarrollaron una metodología Bayesiana para identificar, cuantificar y medir el Riesgo Operacional en diferentes líneas de negocio de la banca comercial. Para lograr los objetivos propuestos, se diseñó un modelo de Red Bayesiana con distribuciones a priori, y a posteriori para estimar la frecuencia y severidad. Las distribuciones a posteriori, según los expertos, permitieron realizar la inferencia sobre la máxima pérdida esperada, para un periodo de 20 días, utilizando el método de simulación de Monte Carlo. Las líneas de negocios analizadas fueron comercialización y ventas, banca minorista, y banca privada, que de forma conjunta representaron el 88,5% de las pérdidas en 2011.

Por último, cabe mencionar otra aplicación en la banca colombiana materializada por [42],”*Diseño de una metodología para la identificación y la medición del riesgo operativo en instituciones financieras* “en la que se brinda una pauta a la hora de conseguir la información para realizar la modelación a través de RB. El investigador sostiene que la información para cada categoría pueden provenir de cuatro fuentes principales: datos históricos al interior de cada entidad, datos sobre eventos de pérdidas en otras entidades de la industria, indicadores de riesgo sobre eventos de pérdidas y juicios de expertos para probabilidades de ocurrencias. Así mismo afirma que son las entidades financieras

importantes de Colombia, las que han empezado a usar metodologías para la identificación y cuantificación del riesgo operacional que puedan dar soporte a la toma de decisiones.

[42], destacan que es importante establecer el horizonte de tiempo en el que se va hacer tal estimación, y que a su caso aplicado en la entidad Bancafé, a la línea Mi Bancafé Empresarial, participaron varias dependencias del banco, donde la recolección de la información se realizó a través de encuestas, siendo esta etapa una de las más importantes en la metodología desarrollada, ya que las variables y probabilidades tienen respaldo en indicadores de riesgo y relaciones definidas para las variables.

Todas las referencias tenidas en cuenta en el desarrollo del estado del arte sirvieron para evidenciar en qué estado está el tema a investigar, siendo de gran aporte para esta tesis y satisfacción a la vez, encontrar hallazgos ya realizados que en su momento hicieron posible ejecutar de manera ordenada y coherente la metodología planteada.

4. Metodología

4.1 Tipo de Estudio

La investigación que tuvo lugar con la realización este proyecto de grado, fue de tipo descriptivo, el cual es una clase de estudio que permite medir, evaluar o recolectar datos sobre distintos conceptos (variables), aspectos, dimensiones o componentes del fenómeno a investigar [43].

En este proyecto también se planteó desarrollar una metodología bayesiana, “la cual especifica un modelo de probabilidad que contenga algún tipo de conocimiento previo acerca de algún parámetro investigativo, por lo que el modelo propuesto condicionará al modelo probabilístico con la intención de relacionar las variables aleatorias mediante un grafo

dirigido” [8].”El modelo propuesto consistió en uno de tipo causal que muestre la capacidad del mismo para predecir como los atributos y variables que han de predecirse dependen entre sí” [1].

Es importante aclarar que la investigación que se proyectó a realizar no fue de tipo experimental, lo cual significa que las variables utilizadas no se emplearon para una finalidad distinta a la propuesta en el proyecto.

De forma general se puede decir que la metodología llevada a cabo se fundamentó principalmente en la recopilación de información teórica de modelos ya implementados en el uso de redes bayesianas para la cuantificación del riesgo operacional en el sector financiero, así como en métodos para identificar los distintos componentes a tener en cuenta en la composición del riesgo objeto de análisis, utilizando criterio de expertos y el uso de base de datos de la entidad siempre y cuando esté disponible y se considere pertinente su utilidad.

4.2 Fases de la Investigación

4.2.1 Fase 1

La fase inicial del proyecto, fue principalmente identificar a través de una revisión de literatura los modelos causales basados en Redes Bayesianas que se han aplicado a la cuantificación de Riesgo Operativo en entidades financieras; ello, para evaluar posteriormente cuál de los modelos investigados se adaptaba mejor a lo que se proponía realizar en el presente trabajo de grado.

De igual modo, en la primera fase se seleccionó la línea de negocio de la entidad financiera en la cual se iba a medir el riesgo operativo. Para esto, se hizo necesario conocer, y comprender como funcionan los procesos al interior de la entidad financiera, que con base a los lineamientos del comité de Basilea fue posible revisar a partir de cada una de las líneas que el organismo internacional ha establecido para tipificar cada área del negocio financiero de los bancos.

4.2.2 Fase 2

Con base a lo establecido por el comité de Basilea en cuanto a la clasificación de los eventos de pérdida que pudieran tener repercusión en el riesgo operativo de una entidad financiera, se consideró la categorización de dichos eventos de acuerdo a los criterios dados por los expertos.

La otra parte en la que estuvo conformada esta fase es la definición de la severidad que los posibles eventos pueden llegar a presentar en el estudio, para esto se establecieron montos para los posibles eventos y se ubicaron tales cantidades en determinados niveles que también pudieron ser determinados y definidos por expertos.

4.2.3 Fase 3

Seguidamente de las dos primeras fases, se requirió identificar indicadores que pudieran generar avisos sobre la existencia de posibles eventos de pérdidas en la entidad financiera. Teniendo en cuenta los lineamientos formulados por el comité de Basilea, se consideraron indicadores para cada subcategoría o para categoría en términos generales, esto según lo que los expertos consideraron mejor.

De igual modo debió definirse niveles para cada tipo de indicador, y en los casos donde hubo lugar a la dependencia de indicadores entre sí, se definió el nivel de relevancia para tal aparte.

4.2.4 Fase 4

En la fase 4, determinó una jerarquización de los indicadores según la categoría de los eventos de pérdidas, para posteriormente revisar el nivel de relación entre el indicador de RO y las posibles ocurrencias en los eventos de pérdida.

4.2.5 Fase 5

Consecutivamente se procedió a construir el modelo causal, para esto se definieron las variables a tener en cuenta, así como las probabilidades a priori utilizando el juicio de expertos. Para definir tales variables, se tuvieron en cuenta las categorías de los posibles eventos de pérdidas y los indicadores para cada categoría, mientras que las probabilidades condicionales, se estimaron posibilidades de ocurrencia dado los distintos niveles en los indicadores previamente definidos.

4.2.6 Fase 6

La validación del modelo construido para este proyecto se efectuó validando las probabilidades condicionales teniendo en cuenta ya sea experiencias ocurridas en otras entidades del sector o información histórica de casos similares, para esto también se consideró tener presente juicios de expertos en la temática.

4.2.7 Fase 7

Esta última etapa presentó como objetivo principal, realizar una simulación de Montecarlo para obtener tal distribución de las pérdidas totales para cada categoría de evento asociado a la línea de negocio objeto de estudio. A partir de la distribución calculada, se cuantificó la provisión total que de forma anual debe cubrir la entidad para hacer frente al riesgo operativo presente en la línea de negocio.

5. Análisis e Interpretación de Resultados

Los resultados que a continuación se exponen en el presente documento corresponden a la aplicación de enfoques ascendentes en la cuantificación del riesgo operativo en una sucursal bancaria de la ciudad de Bucaramanga, dentro de los cuales, se destacaron: el desarrollo de un modelo causal configurado en una Red Bayesiana para identificar de acuerdo a la pregunta problemática qué variables o categorías de pérdidas representan el mayor riesgo de pérdida en una interrelación de factores dadas unas probabilidades condicionales, y por otro lado, la obtención de distribuciones de pérdidas sometidas a una simulación dentro de un modelo estadístico a través del método de Montecarlo, que siendo de carácter no determinista permitió aproximar de forma promediada posibles pérdidas corriendo el modelo propuesto en 10000 iteraciones.

La aplicación de estos enfoques, según expertos se torna compleja si se consideran aspectos como: captura de información que en la mayor parte de las veces resulta complicada hacerla sino hay un sistema de gestión del riesgo consolidado, y sesgos en la información proporcionada por parte de las personas.

Cabe mencionar que, los datos con los que se realizaron las aplicaciones ya mencionadas fueron proporcionados con fines académicos sin ser lo más precisos principalmente por dos razones: procesos internos con gran nivel de confidencialidad sobre su funcionamiento, y disponibilidad de personal adecuado para colaborar en el estudio.

A estos dos últimos aspectos, debe de sumársele que por las condiciones que actualmente se vive por la pandemia producida por COVID-19 las reuniones con los expertos participantes se limitaron en espacio y tiempo por causas de contextos ya conocidas por el mundo entero.

Los resultados obtenidos una vez implementada la metodología plateada se evidencian a continuación:

5.1 Caracterización de la Línea de Negocio Objeto de Estudio

La línea analizada en el estudio fue la de Banca Minorista de una sucursal bancaria de la ciudad de Bucaramanga.

En esta área del negocio bancario, se presenta la siguiente oferta de productos y servicios:

- Retiros y consignaciones
- Pagos de impuestos
- Pagos de servicios públicos
- Apertura de cuentas (de ahorro o corrientes) y entrega de tarjeta débito.
- Cancelaciones de cuentas
- Cancelaciones y/o consignaciones de fiducia.
- Pagos de cheques
- Pagos de créditos

- Pagos de tarjeta de créditos
- Avances de tarjetas de créditos.

La naturaleza de esta línea de negocios según los expertos consultados, radica por lo general en operaciones de ahorradores, clientes particulares y otras formas organizativas como pequeñas y medianas empresas.

Al consultar el criterio de quienes tienen experiencia en el manejo de los procesos internos de la entidad, los mismos sugirieron que al realizar un estudio de riesgo operativo en entidades financieras, tales organizaciones necesitan estimar probabilidades de ocurrencia para los eventos previamente identificados. En este orden de ideas, las valoraciones pueden ser cualitativas, y en contextos de contar con datos históricos, tener en cuenta éstos como valoraciones cuantitativas.

Cabe aclarar que, al no contar con datos históricos para alimentar el diseño de Red Bayesiana desarrollado, se optó por cuantificar los diferentes nodos de la Red Bayesiana con datos subjetivos proporcionados por expertos tanto de la misma sucursal como de otras entidades financieras con experiencia en el tema bancario. Entre ellos, analistas de relacionamiento humano, encargados del área de ciberseguridad, cajeros y analistas de riesgo.

La metodología propuesta para la cuantificación del RO en la sucursal bancaria, abarcó probabilidades de ocurrencias en posibles eventos de pérdidas para el horizonte de tiempo de 1 año.

5.2 Categorización de posibles eventos de pérdidas identificados

De acuerdo a las categorías definidas por el Comité de Basilea para eventos de pérdidas en entidades financieras, y con validación de expertos se tuvieron en cuenta las siguientes:

5.2.1 Fraude Interno

Esta categoría, comprende aquellas pérdidas causadas por acciones de estafa, desfalco, transacciones sin reportar de manera intencional, transacciones sin previa autorización, fraudes en líneas de crédito, depósitos sin efectuar en el sistema, suplantación, falsificaciones, entre otros.

5.2.2 Fraude Externo

Las pérdidas a las que se puede ver expuesta una entidad bancaria por fraude externo son aquellas asociadas con actividades como: asaltos, sobornos, extorsión, piratería informática, hurto de información confidencial.

5.2.3 Fallas en los Sistemas e Interrupción del Negocio

Esta categoría, considera todas aquellas pérdidas a las que se puede exponer la sucursal bancaria por actividades como: daños en el hardware, interrupciones en software, daños potenciales o interrupción en las telecomunicaciones, suspensión en los servicios públicos con incidencia sobre las operaciones del negocio bancario.

5.2.4 Manejo y Ejecución de Procesos

Se consideran en esta sección, pérdidas económicas dadas por malos manejos de los procesos, errores en operaciones transaccionales, mala ejecución del procedimiento de registro de clientes, pérdidas ocasionadas en los activos de los clientes, equivocaciones en el manejo de bases de datos, equivocaciones en los canales de comunicación, fallas en el manejo del sistema contable, mal manejo de procedimientos con proveedores, falla en el procedimiento para gestionar outsourcing.

5.3 Niveles de Severidad para Posibles Eventos de Pérdida

En este punto del proyecto, inicialmente se consultó a los expertos sobre los montos a considerar debido a que cada sucursal presenta un comportamiento distinto, en cuanto al flujo de clientes, y capacidad operativa.

Los juicios proporcionados, permitieron establecer una aproximación de intervalos de pérdidas anuales a los que la sucursal puede verse expuesta por eventos relacionados con las categorías ya descritas.

1. *Nivel 1.* Pérdidas ocasionadas entre \$0 - \$45.000.000
2. *Nivel 2.* Pérdidas ocasionadas entre \$45.000.000 – \$90.000.000
3. *Nivel 3.* Pérdidas ocasionadas entre \$90.000.000-\$145.000.000
4. *Nivel 4.* Pérdidas ocasionadas entre \$145.000.000- \$195.000.000
5. *Nivel 5.* Pérdidas ocasionadas entre \$195.000.000- \$300.000.000

5.4 Indicadores de Riesgo Operativo Identificados

Una vez se identificaron los indicadores de riesgo para cada una de las categorías de eventos de pérdida definidos de manera inicial, se consideró pertinente explorar

subindicadores adicionales para poder comprender de manera más clara y objetiva los indicadores detectados.

A partir de lo anterior, se les solicitó a los directamente implicados en los procesos relacionados con los indicadores a que, según su experiencia y experticia, manifestaran en qué estado podría ubicar a la sucursal objeto de estudio en el cálculo de riesgo operativo en la línea de negocio seleccionada.

5.4.1 Categoría Fraude Interno

Indicador 1. Entrega segura de claves a clientes

Estado: Baja, Media, Alta.

Relación Fraude Interno-Entrega segura de claves a clientes

La relación existente entre ambas variables se logra entender de la siguiente manera: a medida que la entrega de claves a cada cliente sea efectué de una manera segura, se reduce la posibilidad de caer en pérdidas por fraude interno considerando esta vía.

Subindicadores

Subindicador 1. Personas que intervienen en la creación de claves

Estado: Una persona, varias personas.

Relación entre Entrega segura de claves -Personas que intervienen en creación de claves

La relación existente entre quienes intervienen en la creación de claves, y la entrega de las mismas a los clientes puede ser entendida como: mientras menos personas intervengan en la generación de claves en la sucursal bancaria, más segura podría ser la entrega de las contraseñas a los usuarios del sistema.

Subindicador 2. Recepción segura de claves por clientes

Estado: Baja, Media, Alta.

Relación entre Entrega segura de claves-Recepción segura de claves por clientes

En la medida que existan sistemas de comunicación más seguros, y generadores de alerta por parte de la sucursal bancaria de gran calidad, la recepción de claves de igual manera será segura.

Indicador 2. Supervisión

Estado: Si, No.

Relación entre Fraude Interno-Supervisión

Las pérdidas económicas pueden disminuir a causa de fraude interno, si existen altos niveles de supervisión dentro de la sucursal en cada proceso operativo.

Indicador 3. Calidad del personal

Estado: Mala, Regular, Buena.

Los expertos concuerdan en que a medida que los productos y/o servicios ofrecidos en la sucursal sean manejados y proporcionados por personal de buena calidad, la probabilidad de incurrir en fraude interno por medio de esta vía se disminuye.

Subindicadores

Subindicador 1. Personal con antecedentes disciplinarios

Estado: No presenta antecedentes, Presenta antecedentes.

Relación entre Calidad de personal en atención al cliente-Personal con antecedentes disciplinarios.

La calidad del personal en atención al cliente en el mayor de los casos siempre será buena si tal recurso humano para el contexto del negocio bancario, no presenta antecedentes.

Subindicador 2. Nivel de vida del personal

Estado: Bajo, Medio, Alto.

Relación entre Calidad de personal en atención al cliente-Nivel de vida del personal.

A mejor nivel de vida del personal en atención al cliente, generalmente la calidad en prestación de servicio que se brinda utilizando a estos, será de la más alta calidad.

Indicador 4. Manejo seguro de la información de clientes en la línea Banca Minorista.

Estado: Si, No.

Relación entre Fraude Interno-Manejo seguro de la información de clientes en la línea Banca Minorista

Si existe un manejo seguro de la información de los clientes de la sucursal en la línea objeto de estudio, los fraudes internos en la entidad bancaria serán mínimos si se controla tal aspecto.

Indicador 5. Nivel de restricción para pagos a terceros.

Estado: Bajo, Medio, Alto.

Relación entre Fraude Interno-Nivel de restricción para pagos a terceros.

En la medida en que se tenga un sistema de restricciones en el manejo de códigos para pagos a terceros, las posibilidades de incurrir en fraude interno serán menores si se controla esta variable.

5.4.2 Categoría Fraude Externo

Indicador 1. Control del sistema central por parte del superusuario para crear, editar y eliminar usuarios.

Estado: Bajo, Medio, Alto.

Indicador 2. Control del sistema central por parte del superusuario para manipular datos contenidos en archivos de pagos a terceros.

Estado: Bajo, Medio, Alto.

Relación entre Fraude Externo-Control del sistema central por parte del superusuario para manipular datos contenidos en archivos de pago a terceros.

A medida que el superusuario o master tenga mayor control del sistema central para crear, editar y eliminar usuarios, más posibilidades existen para la sucursal bancaria en caer en fraude externo sino se controla tal criterio.

Indicador 3. Exposición a robo o fraude

Estado: Baja, Media, Alta.

Relación entre Fraude Externo-Exposición a robo o fraude

Siempre y cuando la exposición a robo o fraude por parte de la sucursal bancaria sea controlada o en su defecto sea mínima, menor es la posibilidad de que la entidad incurra en pérdidas económicas por fraude externo, si se gestiona mejor tal eventualidad.

5.4.3 Categoría Fallas en los Sistemas e Interrupción del Negocio

Indicador 1. Nivel de concurrencia en el servidor.

Estado: Bajo, Esporádico, Constante.

Relación entre Fallas en los sistemas e interrupción del Negocio-Nivel de concurrencia en el servidor.

Al existir una concurrencia constante los servidores, puede haber más probabilidad de que el sistema falle y se interrumpa el negocio. En este caso, las pérdidas se contarían como lo que se deja de producir si las condiciones fueran las normales.

Indicador 2. Nivel de calidad del hardware

Estado: Bajo, Medio, Alto

Relación entre Fallas en los sistemas e interrupción del Negocio-Nivel de calidad de hardware

En condiciones de baja calidad del hardware bancario, es más probable que el negocio bancario se interrumpa, y se generen condiciones para integrar a otros riesgos operativos en la problemática. Es así, que baja calidad del software produciría pérdidas por fallas en los sistemas e interrupción del negocio.

Indicador 3. Fallas en el suministro eléctrico

Estado: Si, No.

Relación entre Fallas en los sistemas e interrupción del Negocio-Fallas en el suministro eléctrico.

Si se dan fallas en el suministro eléctrico de la sucursal bancaria, aumenta la posibilidad de incurrir en pérdidas por fallas en los sistemas e interrupción del negocio, además que se generan otros tipos de eventos de pérdidas ya descritos.

Indicador 4. Disponibilidad de Firewall

Estado: Si, No.

Relación entre Fallas en los sistemas e interrupción del Negocio-Disponibilidad de Firewall

Al disponerse de un adecuado Firewall en la sucursal bancaria, se disminuye notablemente la posibilidad de caer en pérdidas por fallas en los negocios e interrupción del negocio, y se evita así mismo, la generación de otros tipos de eventos de pérdidas.

5.4.4 Categoría Manejo y Ejecución de Procesos

Indicador 1. Errores en el registro de clientes

Estados: Nunca, Esporádico, Siempre.

Relación entre Manejo y Ejecución de Procesos-Errores en el registro de clientes

En caso dado de que se comentan errores en el registro de clientes de la sucursal bancaria, tales acciones pueden generar mayores posibilidades de que se den pérdidas a raíz de un manejo y ejecución de los procesos.

Subindicadores

Subindicador 1. Envío de claves vía e-mail

Estado:1-15 diarias,16-21 diarias, => 22 diarias

Relación entre Errores en el registro de clientes- Envío de claves vía e-mail

Al disminuir los errores en el envío de claves por correo electrónicos disminuye de igual manera los errores en el registro de clientes.

Subindicador 2. Asignación de claves por teléfono

Estado:0-10 diarias,11-15 diarias, => 16 diarias

Relación entre Errores en el registro de clientes- Asignación de claves por teléfono

Al disminuir los errores en la entrega de claves a través de teléfono, disminuye de igual manera los errores en el registro de clientes.

Indicador 2. Errores en el manejo de Bases de Datos

Estados: Nunca, Esporádico, Siempre.

Relación entre Manejo y Ejecución de Procesos y Errores en el manejo de Bases de Datos

Si persisten errores en el manejo de Bases de Datos, se aumentan las posibilidades de incurrir en pérdidas por manejo y ejecución de procesos en la sucursal bancaria.

5.5 Modelo de Red Bayesiana propuesto para la Sucursal Bancaria Objeto de Análisis

El modelo de Red Bayesiana que se propuso en este trabajo investigativo correspondió a una estructura con nodos alimentados con probabilidades condicionales estimadas mediante juicio o valoraciones de expertos. Tales nodos, se establecieron en referencia a las categorías de eventos de pérdidas previamente identificados, así como indicadores y subindicadores para cada categoría definida.

La estructura de Red Bayesiana para el caso presente, se elaboró mediante el software Hugin Expert Lite 8.9.

La aplicación del modelo estadístico para simular las distribuciones de pérdidas se llevó a cabo utilizando la extensión Risk Simulator de Excel.

5.5.1 Categoría Fraude Interno

En la Tabla 2, se estructuraron las probabilidades condicionales para el nodo raíz entrega segura de claves, que a partir de criterios dados por expertos.

Tabla 2. Probabilidades condicionales para el nodo entrega segura de claves

| Recepción segura de claves Personas en la creación de claves | Baja | | Media | | Alta | |
|---|-----------|-----------------|-----------|-----------------|-----------|-----------------|
| | 1 persona | Varias personas | 1 persona | Varias personas | 1 persona | Varias personas |
| Baja | 0.1 | 0.7 | 0.2 | 0.65 | 0.1 | 0.4 |
| Media | 0.4 | 0.2 | 0.5 | 0.25 | 0.3 | 0.35 |
| Alta | 0.5 | 0.1 | 0.3 | 0.1 | 0.6 | 0.25 |

Nota: * Probabilidades condicionales para estados Baja, Media, y Alta en el procedimiento de entrega segura de claves.

La Tabla 2 expone probabilidades condicionales que se estimaron mediante la valoración cuantitativa de las relaciones dadas entre indicadores y subindicadores. Por ejemplo, la probabilidad condicional de que se dé una entrega segura de claves a nivel medio, cuando al mismo tiempo la recepción segura de las mismas es de nivel bajo y en la creación de claves interviene una sola persona; en este caso la probabilidad condicional dada por expertos fue de 0.4.

En la Tabla 3, se puede evidenciar las probabilidades a priori dadas por expertos para el nodo personas que intervienen en la creación de claves.

Tabla 3. *Probabilidades para Personas que intervienen en la creación de claves*

| Estado | Probabilidad |
|------------------------|---------------------|
| Una Persona | 0.95 |
| Varias Personas | 0.05 |

Nota: * Probabilidades a priori para estados de una persona, y varias personas en el procedimiento de creación de claves.

Para la variables de personas que intervienen en la creación de claves, se obtuvo por parte de los expertos que en el 95% de las veces una sola persona interviene a manera de vigilancia y control sobre el procedimiento de creación de claves, mientras un 5% de las veces puede darse la ocasión de que intervengan más de uno sin ser la cantidad excesiva ya que pueden darse eventualidades ajenas al procedimiento, es escaso ese momento pero según los juicios proporcionados resulta importante tener en cuenta la probabilidad dada.

En la Tabla 4, se estructuró el nodo recepción segura de claves por clientes proporcionando para cada estado, la probabilidad a priori para cada uno de ellos.

Tabla 4. *Probabilidades para Recepción segura de claves por clientes*

| Estado | Probabilidad |
|---------------|---------------------|
| Bajo | 0.20 |
| Medio | 0.30 |
| Alto | 0.50 |

Nota: * Probabilidades a priori para estados Bajo, Medio, y Alto en el procedimiento de recepción segura de claves por clientes.

Dadas las opiniones de expertos en cuento a la variable recepción segura de claves por clientes, se observó en la Tabla 4 que, según las valoraciones dadas, en el 20% de los casos es posible tener una baja recepción segura de claves asignadas por parte de los clientes, esto debido a que la sucursal bancaria no puede controlar el correo, ni el dispositivo móvil donde podrían llegar los códigos establecidos para cada usuario. De igual manera, podría darse un 30% de recepción segura en estado medio y un 50% en estado alto, ya que las condiciones de la entidad financiera garantizan la emisión segura de las contraseñas creadas para cada perfil.

Es posible observar en la Tabla 5, probabilidades a priori estimadas para la variable personal con antecedentes disciplinarios.

Tabla 5. *Probabilidades para Personal con antecedentes disciplinarios*

| Estado | Probabilidad |
|---------------------------------|---------------------|
| No presenta antecedentes | 1 |
| Presenta antecedentes | 0 |

Nota: * Probabilidades a priori para estados No presenta antecedentes y presenta antecedentes en el procedimiento de selección de personal.

En la Tabla 5, se pudo observar que los expertos proporcionaron una valoración absoluta para No presenta antecedentes. Esta razón según criterios subjetivos de los mismos se debe a que, los empleados de la sucursal deben ser ejemplo en el sistema financiero por lo

que no presentar antecedentes de tipo disciplinario constituye un factor importante al momento de ser seleccionado.

La variable nivel de vida del personal operativo en la línea de negocio Banca Minorista, puede observarse de forma detallada en la Tabla 6, donde para cada estado del nodo en mención se establecieron probabilidades a priori para cada uno de ellos.

Tabla 6. Probabilidades para Nivel de vida del personal

| Estado | Probabilidad |
|---------------|---------------------|
| Bajo | 0.15 |
| Medio | 0.8 |
| Alto | 0.05 |

Nota: * Probabilidades a priori para estados Bajo, Medio, y Alto en el nivel de vida de quienes manejan los procesos internos de la sucursal.

De la Tabla 6 se observó que, en un 80% de las veces el personal de la sucursal presenta un nivel de vida medio. La importancia de esta variable se fundamenta en que, según la opinión de los expertos un nivel de vida bajo del personal podría influir en la toma de malas decisiones por parte de los colaboradores que al final pueden poner en riesgo el capital tanto de la entidad como de los clientes. Lo anterior es lo estándar en una línea de negocio como la analizada en este trabajo.

En la Tabla 7, se evidenciaron las probabilidades a priori dadas por los expertos para cada estado de la variable supervisión.

Tabla 7. *Probabilidades para Supervisión*

| Estado | Probabilidad |
|---------------|---------------------|
| Si | 0.95 |
| No | 0.05 |

Nota: * Probabilidades a priori para estados Si, y No en la supervisión de procesos internos de la sucursal.

En el 95% de las ocasiones, existe un 95% de supervisión sobre los procesos que tienen lugar en la línea de negocio de Banca Minorista de la sucursal analizada, el otro 5% obedece según los expertos a eventos en los que puede faltar ya sea por simple omisión o responsabilidad directa de quien delega alguna función respecto al proceso a ejecutar.

Para la variables o nodo manejo seguro de la información de clientes, en la Tabla 8, establecieron probabilidades a priori para cada estado del nodo.

Tabla 8. *Probabilidades para Manejo seguro de la información de clientes*

| Estado | Probabilidad |
|---------------|---------------------|
| Si | 0.95 |
| No | 0.05 |

Nota: * Probabilidades a priori para estados Si, y No en el manejo seguro de la información de procesos internos de la sucursal.

Una vez consultados a los expertos en el caso que corresponde al manejo seguro de la información resultante de los procesos internos de la sucursal, los mismo indicaron que en un 95% de las veces el negocio bancario requiere de un alto control de este tipo de información y que si bien es riguroso en tal aspecto todavía hace falta mejorar para evitar que por ejemplo casos de falsificación o suplantación de identidad puedan darse, por tal motivo asignaron un 5% al estado No en la variable descrita.

Para la variable nivel de restricción de pagos a terceros, en la Tabla 9 se pudieron estimar las probabilidades a priori para cada estado dadas por los expertos.

Tabla 9. Probabilidades para Nivel de restricción para pagos a terceros

| Estado | Probabilidad |
|---------------|---------------------|
| Bajo | 0.10 |
| Medio | 0.10 |
| Alto | 0.80 |

Nota: * Probabilidades a priori para estados Bajo, Medio y Alto en el nivel de restricción para pagos a terceros en la sucursal.

Según lo expuesto en la Tabla 9 se evidenció que, en la mayoría de los caso existe un alto nivel de restricción para pagos a terceros, esto es un 80%. El sector bancario, según lo manifestado por los expertos ha tenido en los último 20 años un gran avance en controlar el sistema de pagos a terceros mediante filtros basados en códigos para convenios que permiten garantizar el destino seguro de la transacción, así como el registro cruzado del movimiento contable el sistema maestro central de la entidad.

Una vez definidas tales probabilidades a priori para cada nodo, se estableció una tabla de probabilidades condicionales para establecer de manera a posteriori la probabilidad de caer en riesgo sea 1,2,3,4 o 5, por causa de fraude interno una vez interrelacionados las variables mediante la relación indicadores-subindicadores-estados finales de fraude interno.

Las probabilidades condicionales proporcionadas se pueden visualizar en los apéndices A, B, C, D, E y H.

En la Figura 3 se puede observar la estructura de la RB diseñada para la categoría fraude interno, y así mismo, las probabilidades a posteriori resultantes del proceso de

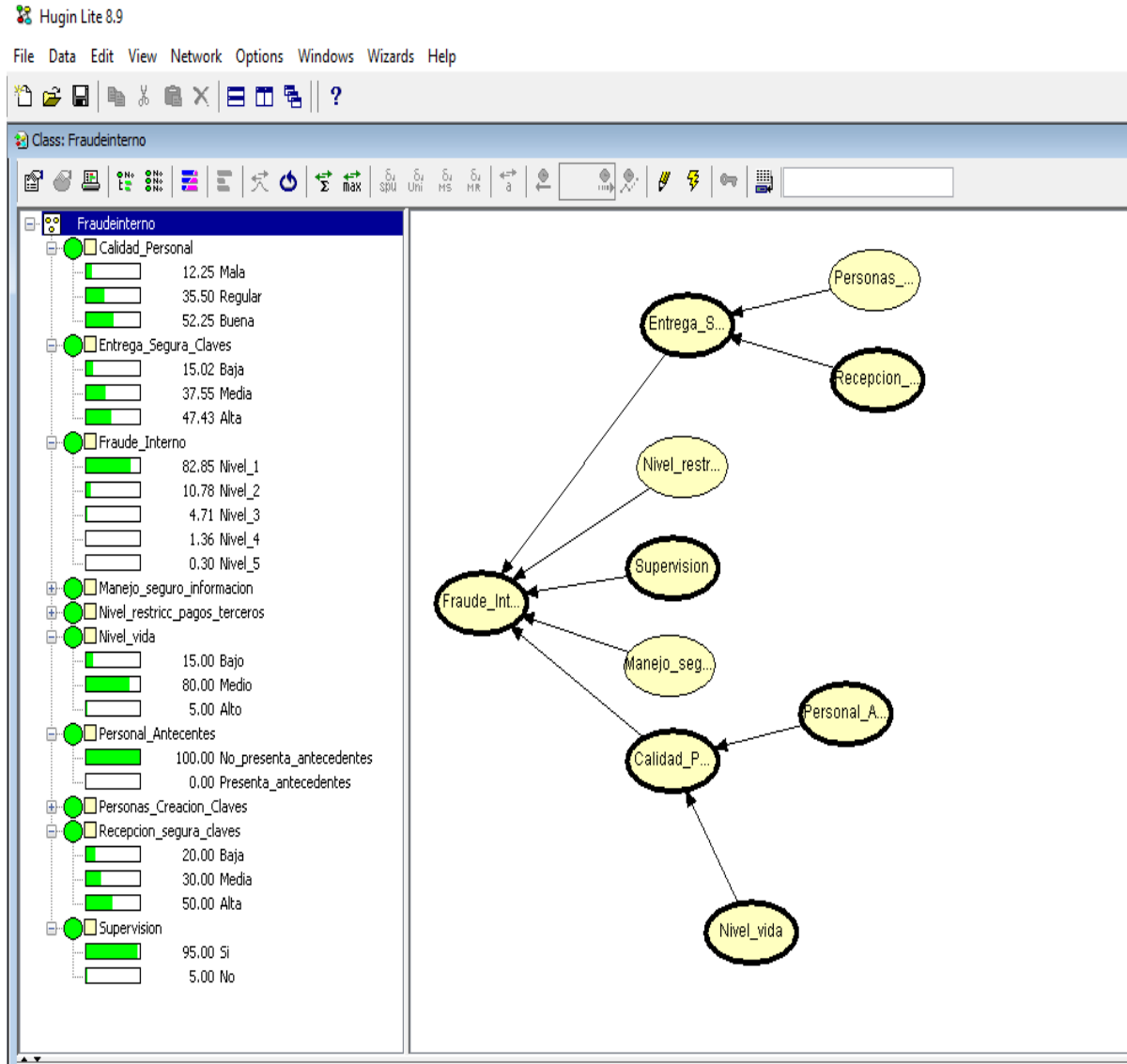
propagación a través de los nodos del grafo mediante las interrelaciones previamente definidas.

Las variables que se pueden observar en la RB para fraude interno, correspondieron a elementos previamente definidos con orientación de los especialistas en Riesgo Operacional en entidades bancarias. Es importante mencionar que, se utilizaron probabilidades tanto de naturaleza a priori como de naturaleza condicional.

Los resultados pueden interpretarse estableciendo interrelaciones de los atributos a medida en que crecen o disminuyen de manera probabilística su posible ocurrencia dentro del contexto estudiado.

Las variables que corresponden a un nivel de 100%, fueron determinadas de esa manera ya que, fueron requerimientos que se establecieron así y son partes del reglamento interno de selección de personal de la empresa. Ejemplo de lo anterior es el estado de antecedentes con un nivel de 100%, esto se debe a que, para la sucursal el que el posible colaborador no presente antecedentes de forma total es un requisito obligatorio para ingresar a laborar dentro de ella.

Deben de interpretarse las barras en verdes como variaciones de cada variable dependiendo de las relaciones existentes entre las variables internas del mismo modelo, todo buscando el nodo principal que fue el nodo de fraude interno.

Figura 4. Red Bayesiana para fraude interno.

Nota: * Resultados de la Red Bayesiana para la categoría fraude interno dado un conjunto de probabilidades a priori y condicionales para cada nodo por parte de expertos.

En la Figura 3, se observó que, bajo las condiciones y parámetros dados por los expertos, la sucursal bancaria presentó un riesgo nivel 1 al 82.85%. Lo anterior significa que, dada la caracterización para la severidad de cada nivel, la entidad está más expuesta a tener pérdidas entre \$0 y \$45.000.000 que a niveles superiores. El contexto resultante, se produjo

debido variables como recepción segura de claves y entrega segura de claves, las cuales en caso más exactos de un estudio posterior seguramente podrían obtenerse resultados más precisos.

Los niveles restantes, aunque se evidenciaron riesgos menores o igual a 10.78% reflejan el manejo riguroso que le he dado la entidad bancaria a eventos que podrían comprometer cuantificaciones de perdidas mayores afectando la rentabilidad del banco.

5.5.2 *Categoría Fraude Externo*

En la Tabla 10, se configuraron las probabilidades a priori para los estados de la variable control del sistema central por parte del superusuario para crear, editar y eliminar usuarios.

Tabla 10. *Probabilidades para control del sistema central por parte del superusuario para crear, editar y eliminar usuarios*

| Estado | Probabilidad |
|---------------|---------------------|
| Bajo | 0.10 |
| Medio | 0.20 |
| Alto | 0.70 |

Nota: * Probabilidades a priori para estados Bajo, Medio y Alto en el control del sistema por parte del superusuario para crear, editar, y eliminar usuarios.

En la Tabla 10, se evidenciaron las probabilidades a priori de ocurrencia para los niveles de control por parte del superusuario para manipular el sistema. Los expertos afirmaron que existe una probabilidad del 70% de que se de un control de nivel alto sobre el superusuario, un control de nivel medio al 20% y un control a nivel bajo tan solo el 10%, algo característico de la sucursal objeto de estudio.

En la Tabla 11, se pueden observar probabilidades a priori que se proporcionaron para los estados de la variable control del sistema central por parte del superusuario para manipular datos contenidos en archivos de pagos a terceros.

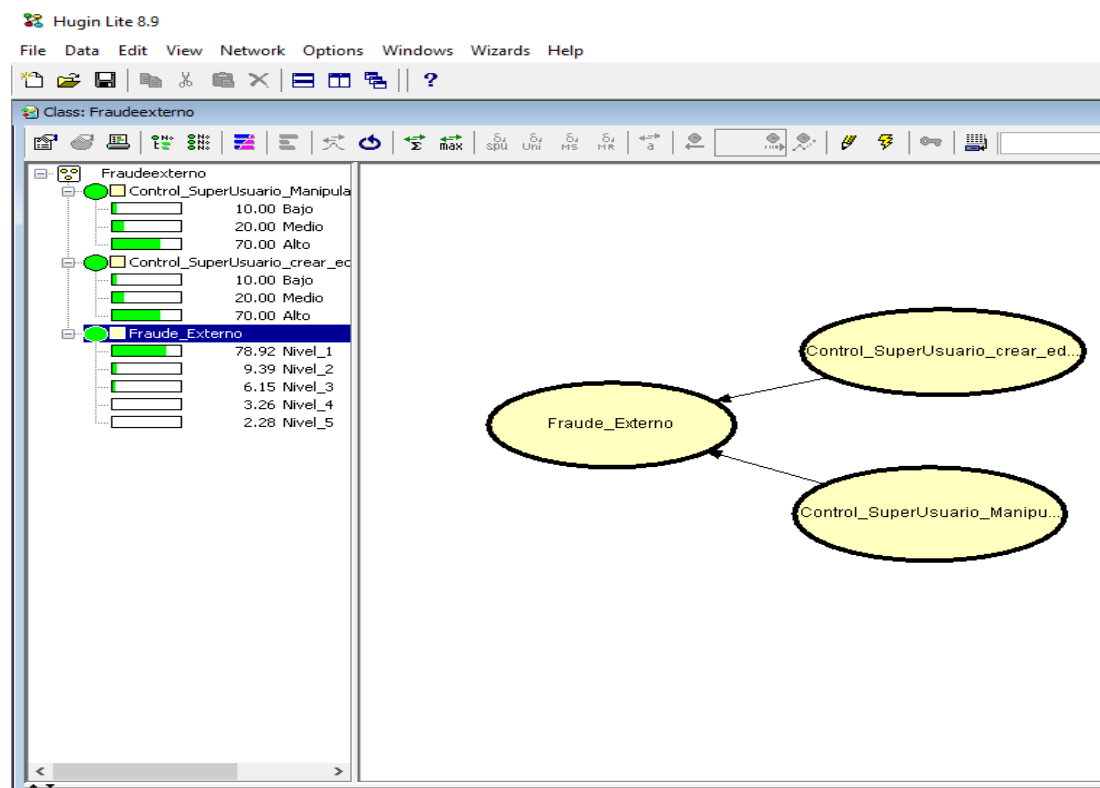
Tabla 11. Probabilidades para control del sistema central por parte del superusuario para manipular datos contenidos en archivos de pagos a terceros

| Estado | Probabilidad |
|---------------|---------------------|
| Bajo | 0.10 |
| Medio | 0.20 |
| Alto | 0.70 |

Nota: * Probabilidades a priori para estados Bajo, Medio y Alto en el control del sistema por parte del superusuario para manipular datos en archivos de pagos a terceros.

Se reflejó al igual que en el caso anterior, una valoración del 70% para el control del manejo que el superusuario hace sobre el sistema para evitar la manipulación de datos contenidos en archivos de pagos a terceros. En la Tabla 11, de igual manera cabe mencionar que se realizaron valoraciones para el mismo caso de probabilidades a priori para el control a nivel medio y bajo de 20% y 10% respectivamente.

El fraude externo, correspondió a todos aquellos factores que pueden generar riesgo de pérdidas económicas para la sucursal bancaria objeto de estudio, y que a su vez pueden ocurrir al exterior del sistema de la misma entidad, pero guardando siempre la relación de quien maneja el sistema o superusuario con el control master o sistema maestro de información bancario.

Figura 5. Red Bayesiana para fraude externo

Nota: * Resultados de la Red Bayesiana para la categoría fraude externo dado un conjunto de probabilidades a priori y condicionales para cada nodo por parte de expertos.

Para el análisis de los resultados una vez corrida la RB para la categoría fraude externo, se hace necesario contextualizar al lector que fueron variables relacionadas con aquella manipulación que puede tener el sistema por parte de quien lo controla, pero en casos externos al sistema de información de la sucursal.

Una vez observada la Figura 4 se pudo inferir que, por causa de fraude externo bajo los parámetros dados por los expertos, la sucursal bancaria se encontró expuesta a un nivel 1 al 78.92%, es decir, a caer en pérdidas comprendidas entre \$0 y \$45.000.000. Una vez socializados los resultados a los conocedores del tema, se explicó que el darle aun más rigurosidad al estado de control medio para ambas variables, esto permitiría disminuir el porcentaje de riesgo en los niveles superiores de posibles pérdidas.

Las variables condicionales que se incorporaron al modelo de RB desarrollados se pueden observar en el apéndice G.

5.5.3 *Categoría Fallas en los Sistemas e Interrupción del Negocio*

En el apéndice F, se puede observar las probabilidades condicionales para la categoría fallas en los sistemas e interrupción del negocio.

En la Tabla 12, se estimaron probabilidades a priori sobre los estados de la variable disponibilidad de firewall en la sucursal bancaria.

Tabla 12. *Probabilidades a priori de disponibilidad de firewall*

| Estado | Probabilidad |
|---------------|---------------------|
| Si | 0.95 |
| No | 0.05 |

Nota: * probabilidades a priori para estados Si y No de la variable disponibilidad de firewall en la sucursal bancaria.

Las valoraciones dadas por parte de los expertos, indicaron que en un 95% siempre está disponible un sistema firewall para evitar ciberataques al sistema de información de la entidad. El 5% considerado como No, aunque es algo grande para la rigurosidad de la sucursal se determinó para sobreestimar casos en los que puede según quienes tienen experiencia en el sector, tal sistema de protección pueda fallar.

En la Tabla 13, se establecieron las probabilidades a priori para los estados de la variable nivel de concurrencia del servidor dadas por expertos.

Tabla 13. Probabilidades a priori para nivel concurrencia del servidor

| Estado | Probabilidad |
|------------|--------------|
| Bajo | 0.1 |
| Esporádico | 0.6 |
| Constante | 0.3 |

Nota: * probabilidades a priori para estados Bajo, Esporádico y Constante de la variable nivel de concurrencia del servidor.

Lo observado en la Tabla 13 indicó que los especialistas creen que, en un 60% el servidor principal donde se ejecutan los procesos de la línea de negocio analizada es concurrido de forma esporádica. Un 30% de las veces lo está de manera constante, y un 10% concurrido a un nivel bajo, todo lo anterior en una jornada de trabajo normal.

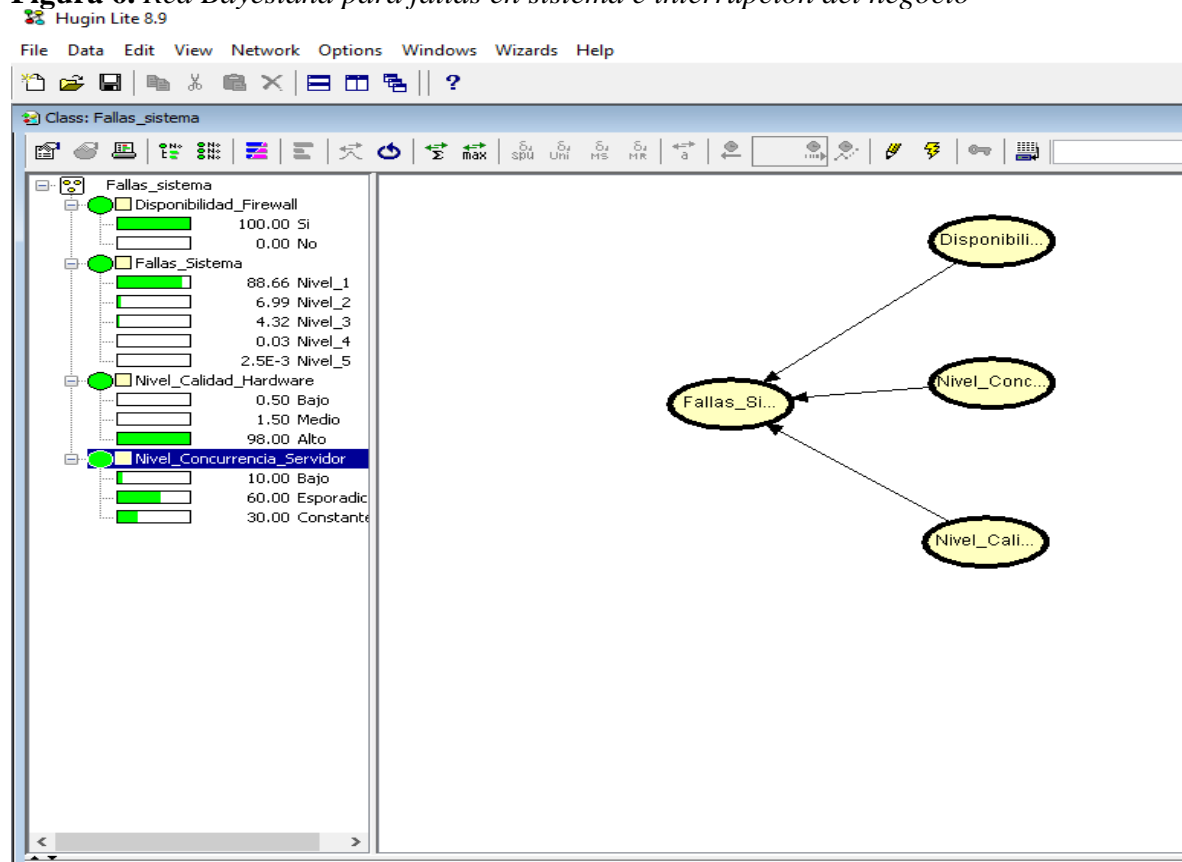
En la Tabla 14, para los estados de la variable nivel de calidad del hardware se determinaron probabilidades a priori.

Tabla 14. Probabilidades a priori del nivel de calidad del hardware

| Estado | Probabilidad |
|--------|--------------|
| Bajo | 0.005 |
| Medio | 0.015 |
| Alto | 0.98 |

Nota: * probabilidades a priori para estados Bajo, Medio, y Alto de la variable nivel de calidad del hardware en la sucursal bancaria.

A partir de la Tabla 14, se puede resaltar una característica importante de la entidad bancaria estudiada, esto es, el gran nivel de calidad en hardware que tiene en todos y cada unos de sus equipos para llevar a cabo el negocio bancario. Los expertos indicaron, que la probabilidad de que tales equipos sean de alta calidad es del 98%. Los niveles Bajo y Medio, tan solo son de 0.5% y 1.5% respectivamente.

Figura 6. Red Bayesiana para fallas en sistema e interrupción del negocio

Nota: * Resultados de la Red Bayesiana para la categoría fallas en sistema e interrupción del negocio dado un conjunto de probabilidades a priori y condicionales para cada nodo por parte de expertos.

La Figura 5, reflejó que la sucursal bancaria dadas las valoraciones y criterios por parte de los expertos, está expuesta a pérdidas de nivel 1 en un 88.66%, o del mismo modo que las pérdidas que podría tener por causa de fallas en sistemas podrían estar entre \$0 y \$45.000.000, tal riesgo según los expertos puede estar dado en gran parte por un nivel de concurrencia constante en el servidor al 30%.

5.5.4 Categoría Manejo y Ejecución de Procesos

En el apéndice I, puede observarse las probabilidades condicionales dadas por expertos para el nodo principal manejo y ejecución de procesos para cada nivel, dados unos eventos posibles de pérdidas.

La Tabla 15, muestra las probabilidades a priori dadas para los estados de la variable envío de claves vía e-mail.

Tabla 15. Probabilidades para envío de claves vía e-mail

| Estado | Probabilidad |
|---------------|--------------|
| 1-15 diarias | 0.75 |
| 16-21 diarias | 0.15 |
| =>22 diarias | 0.1 |

Nota: * probabilidades a priori para estados 1-15 diarias, 16-21 diarias y =>22 diarias, equivalentes a claves enviadas de manera errónea desde la entidad bancaria vía e-mail.

Para comprender las Tabla 15, debe hacerse de la siguiente manera: los expertos indicaron que en un 75% existe la posibilidad de que generen errores en claves enviadas por vía e-mail en un intervalo de 1-15 diarias.

En la Tabla 16, se estimaron de forma organizada las probabilidades a priori para los estados de la variable envío de claves vía teléfono.

Tabla 16. Probabilidades a priori para envío de claves vía teléfono

| Estado | Probabilidad |
|---------------|--------------|
| 0-10 diarias | 0.8 |
| 11-15 diarias | 0.1 |
| =>16 diarias | 0.1 |

Nota: * probabilidades a priori para estados 0-10 diarias, 11-15 diarias, y =>16 diarias, equivalentes a claves enviadas de manera errónea desde la entidad bancaria vía teléfono.

La comprensión de la Tabla 16, debe hacerse al igual que en la Tabla 15, es decir en un 80% los especialistas en el tema indicador que se podrían generar claves con errores enviadas por vía telefónica.

Los expertos de igual manera, indicaron que el rango para el caso de la sucursal bancaria en estudio comprende cantidades bajas por la alta precisión de los procedimientos pero que para fines del estudio debería de considerarse la mayor probabilidad para el estado 0-10 siendo más coherentes con la realidad de la entidad bancaria.

En la Tabla 17, se establecieron probabilidades condicionales para la variable errores en el registro de clientes.

Tabla 17. Probabilidades condicionales para nodo errores en el registro de clientes

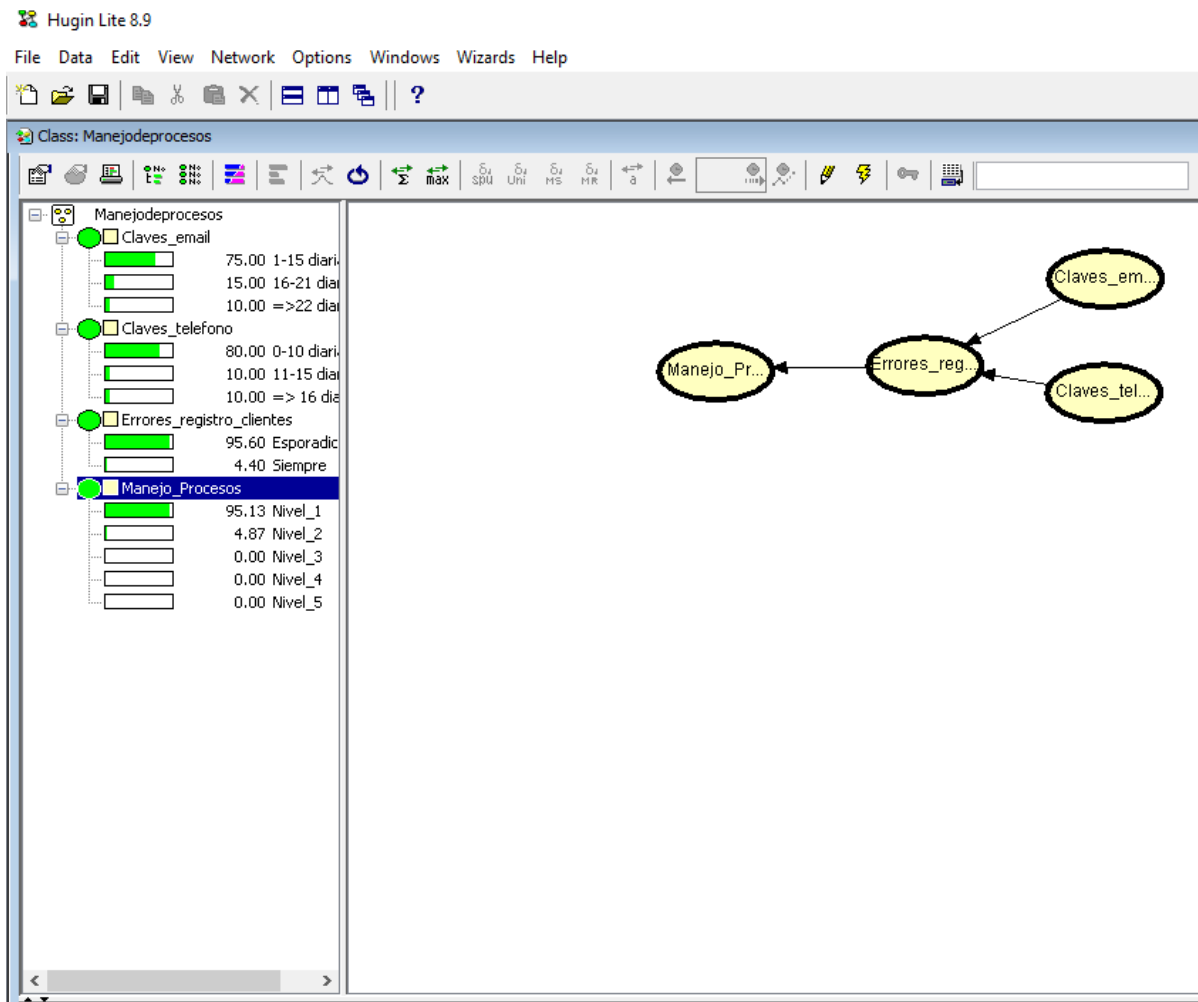
| Claves enviadas vía teléfono | 0-10 diarias | | | 11-15 diarias | | | =>16 diarias | | |
|------------------------------|--------------|---------------|--------------|---------------|---------------|--------------|--------------|---------------|--------------|
| | 1-15 diarias | 16-21 diarias | =>22 diarias | 1-15 diarias | 16-21 diarias | =>22 diarias | 1-15 diarias | 16-21 diarias | =>22 diarias |
| Claves enviadas vía e-mail | | | | | | | | | |
| Esporádico | 0.95 | 0.97 | 0.98 | 0.95 | 0.97 | 0.98 | 0.95 | 0.97 | 0.98 |
| Siempre | 0.05 | 0.03 | 0.02 | 0.05 | 0.03 | 0.02 | 0.05 | 0.03 | 0.02 |

Nota: * probabilidades condicionales para los estados relacionados con el nodo errores en el registro de clientes de la sucursal bancaria objeto de estudio.

Una manera de leer la Tabla 17, corresponde a la siguiente interpretación: la probabilidad condicional de que se de un registro erróneo de clientes esporádico, cuando se envían claves vía teléfono con errores en un intervalo de 0 a 10 claves diarias, y al mismo tiempo son enviadas claves vía e-mail con errores en un intervalo de 1-15 diarias, es de 95%.

En la Figura 6, es posible observar la estructura de la RB para la categoría manejo y ejecución de procesos, de igual manera las relaciones existentes entre indicadores y subindicadores previamente definidos.

Figura 7. Red Bayesiana de manejo y ejecución de procesos



Nota: * Resultados de la Red Bayesiana para la categoría fallas en sistema e interrupción del negocio dado un conjunto de probabilidades a priori y condicionales para cada nodo por parte de expertos.

Al analizar al Figura 6, se pudo inferir que la entidad bancaria estudiada se encontró expuesta a un riesgo de nivel 1 al 95,13%. Lo anterior significa que, en caso de caer en

perdidas por manejo y ejecución de procesos, sería en un gran parte claves enviadas vía e-mail entre 1-15 diarias, y claves enviadas vía teléfono entre 0-10 diarias. Lo explicado por expertos, se fundamenta en que, si bien los canales de la entidad son vigilados con tecnología de punta, los puntos de recepción del cliente pueden estar expuesto a factores externos de fraude.

De igual manera se indicó que, en estudio más exhaustivos y precisos, es posible determinar con mayor exactitud las probabilidades para cada evento.

5.6 Validación de Modelo de Red de Bayesiana

Al consultar a los expertos sobre el modelo desarrollado, los mismos informaron que hacer una validación sobre la carencia de datos históricos no representaba un criterio con objetividad. Al respecto, lo sugerido fue establecer intervalos de montos de pérdidas para luego encontrar probabilidades de ocurrencia de pérdidas dentro de tales rangos. Al final lo explicado por los especialistas se fundamentó en que, las probabilidades obtenidas eran coherentes con los datos sugeridos inicialmente por ellos, pero con estudios posteriores y más adentro de la organización las redes bayesianas solo necesitarían de actualización de probabilidades.

5.7 Distribución de Pérdidas agregadas

Una vez encontrados las probabilidades de pérdidas para cada categoría utilizando la Red Bayesiana construida, y siguiendo los criterios de los expertos, se calcularon distribuciones de pérdidas para cada categoría teniendo en cuenta un modelo estadístico en el que mediante el método de Montecarlo fue posible cuantificar de manera aproximada

valores económicos a considerar para cubrir eventos característicos de cada categoría simulada con datos suministrados por expertos.

El modelo desarrollado en el presente trabajo de investigación, tuvo como propósito encontrar el valor en riesgo o OpVar (Operational Value at Risk), el cual según estudios previos y expertos en la temática coincide con el percentil 95 de la distribución de pérdidas y se considera aquella cantidad máxima que puede estar en riesgo por uno u otro posible evento de pérdida.

De igual manera, se aplicó para el desarrollo del modelo propuesto, el algoritmo de recursividad de *Panjer*.

El algoritmo referenciado, posibilita la construcción una distribución de pérdidas agregadas a partir de dos distribuciones asociadas a cada celda (i,j) [44].

Partiendo de una variable aleatoria de conteo N con función de probabilidad $p(n)=P(N=n)$, que corresponde a la distribución de frecuencia de pérdidas, y así mismo, se considera una variable aleatoria continua X , que corresponde a la severidad de la pérdida de tal evento cuando sucede [44].

El algoritmo de *Panjer*, está fundamentado en el calculo de una distribución compuesta realizando convoluciones en el que, además se tiene en cuenta que la distribución de la adición de dos variables aleatorias continuas que son independientes puede determinarse mediante una convolución [44].

Las pérdidas agregadas son de la siguiente manera:

$$S = X_1 + X_1 + \dots + X_N = \sum_{i=1}^N X_i$$

Donde $X_i = 0$, cuando $N=0$.

Generalmente se plantean los siguientes supuestos:

1. X_1, X_2, \dots corresponden a variables que son aleatorias e idénticamente distribuidas

2. Las variables N, X_1, X_2 , son independientes.

Las distribuciones de frecuencia y severidad constituyen el centro del modelo planteado, y fueron utilizadas para estimar la pérdida agregada para la celda (i,j) en un horizonte específico de estudio, que generalmente es un año [44].

Se estableció un modelo con distribuciones tanto de severidad como de frecuencia para cada categoría simulada.

Para la distribución de frecuencia, los expertos indicaron que podría haberse tenido como referencia las distribuciones Poisson o Binomial, mientras que para la distribución de severidad la distribución de probabilidad que debería tenerse en cuenta es la Logarítmica Normal (Lognormal), esto porque es un tipo de distribución de cola pesada que permite sobreestimar las pérdidas que pueden tener lugar en el riesgo operacional, es decir, por no estar acotada de forma exponencial permite con más proximidad determinar el valor del OpVar.

Para la distribución de frecuencia se eligió Poisson, y para la distribución de severidad Lognormal.

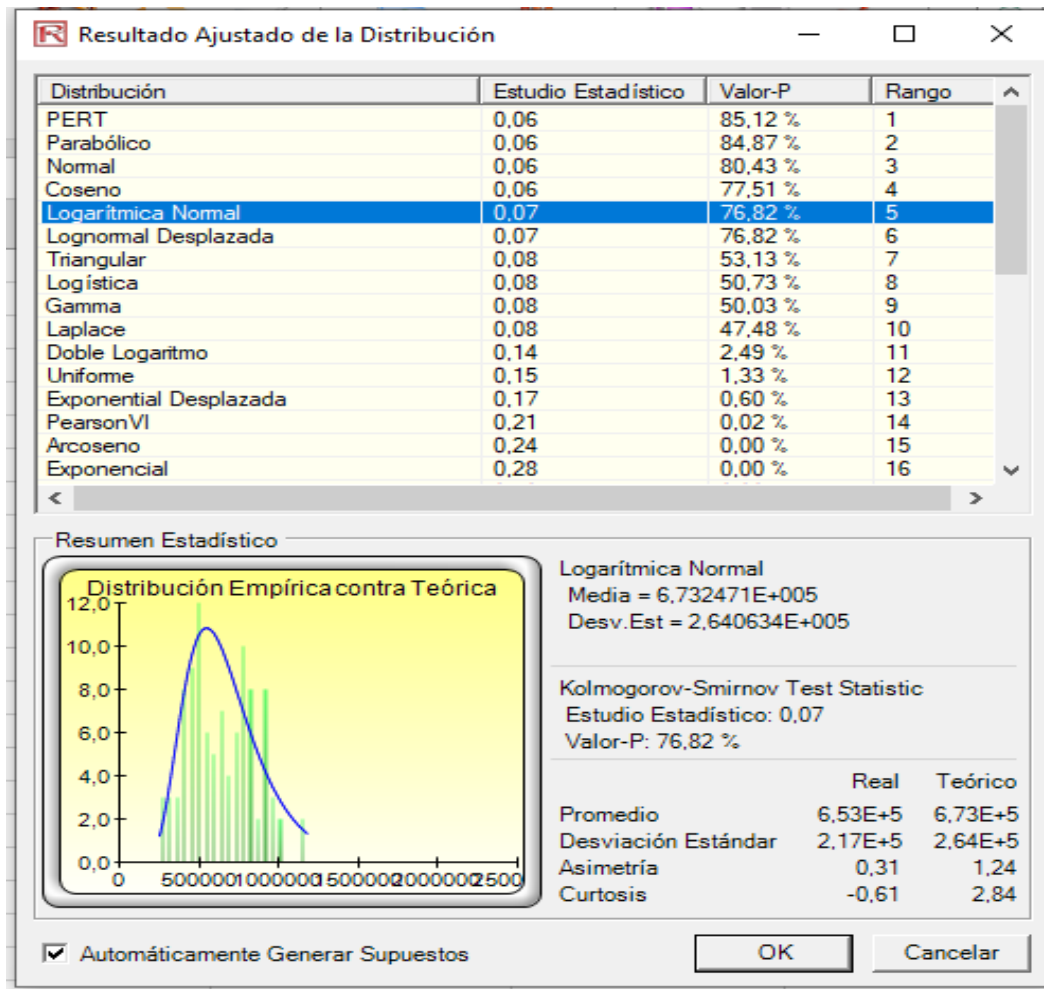
Para ajustar cada una de las distribuciones de los datos dados por expertos, se realizó un ajuste para distribuciones continuas con el test estadístico Kolmogorov-Smirnov, teniendo en cuenta un p-value superior a 0,5.

5.7.1 Ajuste de Distribución de Severidad de la Categoría Fraude Interno

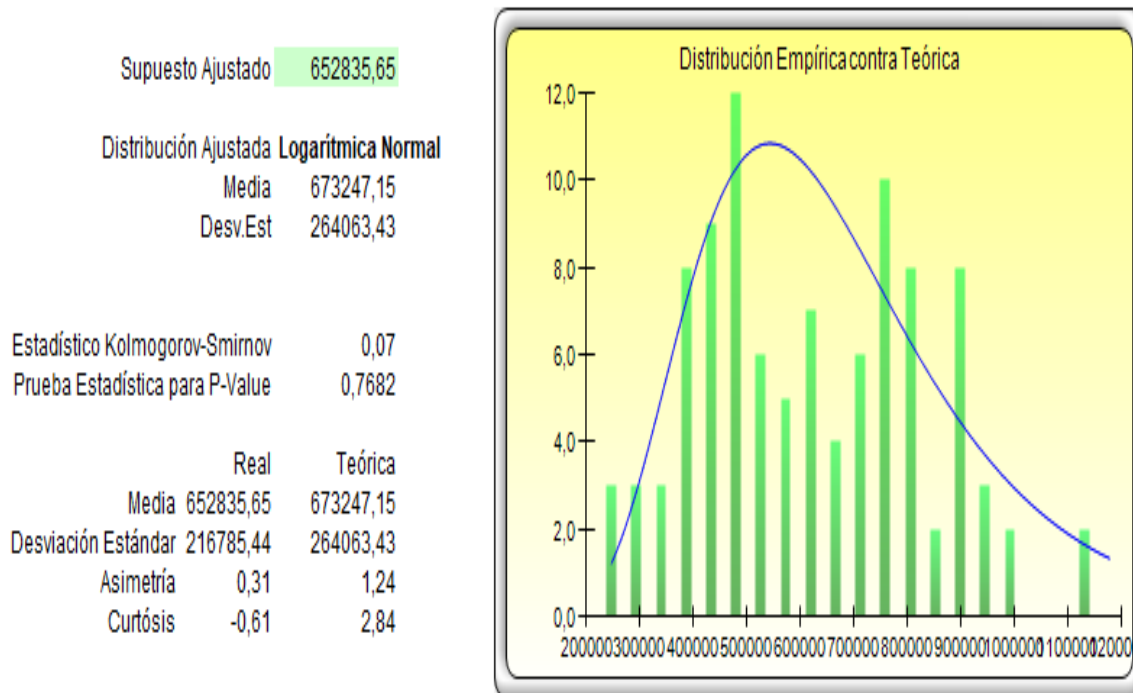
En la Figura 7, considerando las recomendaciones dadas por los expertos, y según experiencias ya investigadas se prefirió elegir la distribución Lognormal por dos razones: la

primera es porque su P-valúe es >0.5 , y la segunda corresponde a que, por ser una distribución de probabilidad de cola pesada, logra sobrestimar las perdidas agregadas, esto porque exponencialmente no se encuentra acotada.

Figura 8. P-value para distribución fraude interno

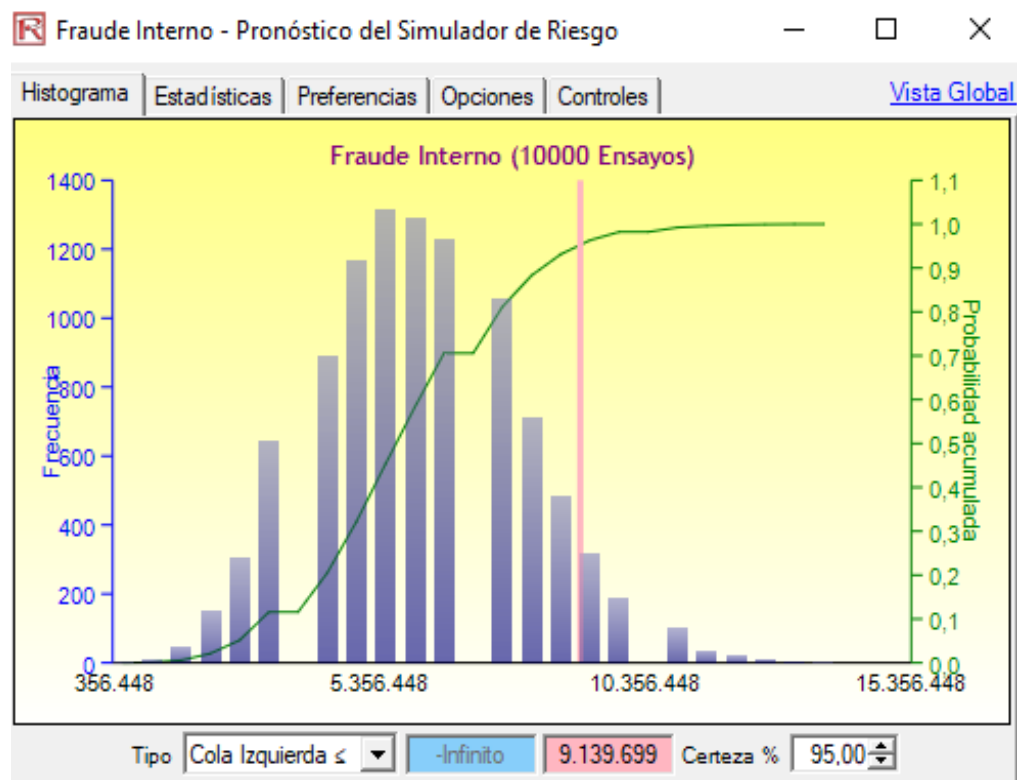


Para fraude interno puede verse que la serie de datos se ajusta más a otras distribuciones de probabilidad, pero la Lognormal fue la recomendada por los expertos por sobrestimar los costos de pérdida posibles para cada categoría.

Figura 9. Distribución de datos de severidad ajustada a la distribución Lognormal para

Los resultados obtenidos a partir del ajuste de distribución evidenciado en la Figura 7, permitieron demostrar que los registros se pueden ajustar para el modelo estadístico de pérdidas agregadas con una distribución Lognormal, pues su P-value es >0.5 , es decir 0.7682. La Figura 8, representa la distribución ajustada a la distribución Lognormal a la que se ajustó la distribución de severidad para la categoría fraude interno.

De igual manera, arrojó un supuesto ajustado a la media real de los datos que sirvió para alimentar las convoluciones del modelo.

Figura 10. Simulación de categoría fraude interno

La Figura 9, evidenció los resultados obtenidos de la simulación para la categoría fraude interno que, a 10000 iteraciones, dio como resultado para el OpVar una aproximación del valor en riesgo de \$9.139. 699.Cabe mencionar que, el OpVar es el valor que correspondió al percentil 95.

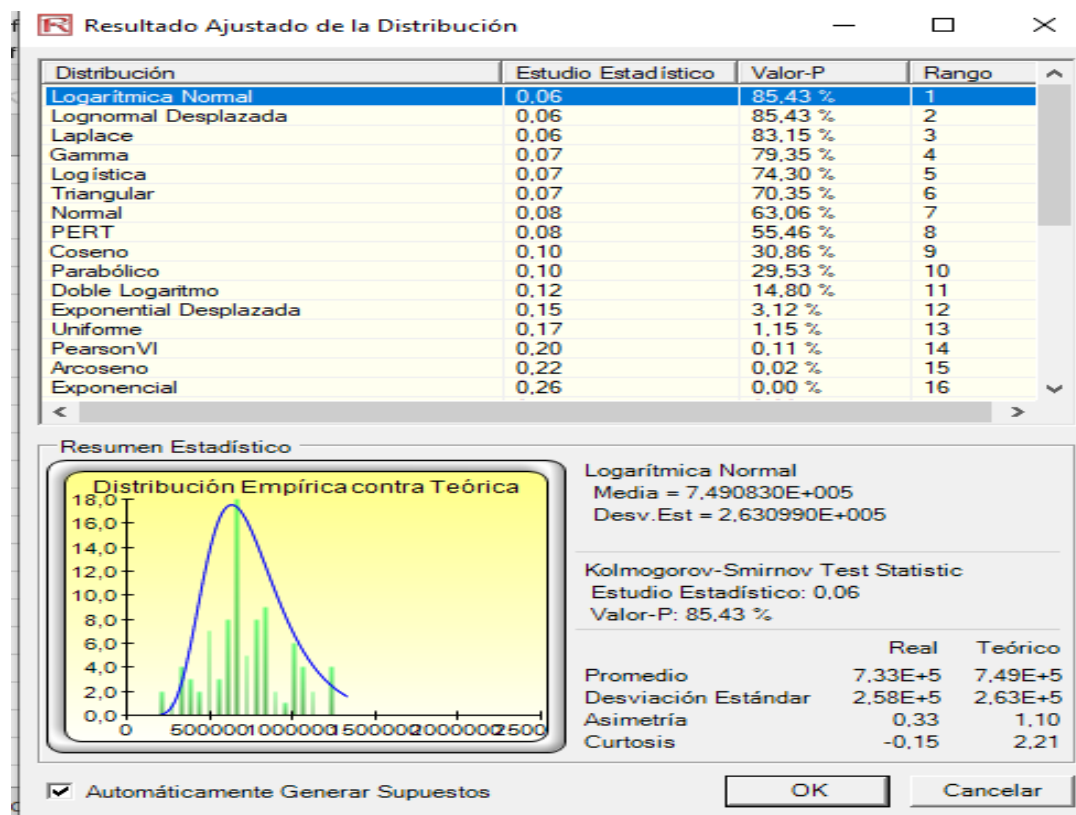
5.7.2 Ajuste de Distribución de Severidad de la Categoría Fraude Externo

En la Figura 10,se puede observar que distribuciones se ajustan de mejor manera a la distribución de severidad dada para la categoría de fraude externo.

Cabe mencionar que si bien en este caso la distribución de los datos se ajustó a una Lognormal,pudo haberse ajustado a otra pero la Lognormal todavía fuese la utilizada en el

modelo debido a que es un parametro recomendado ya que al ser una distribución de probabilidad de cola pesada sobrestima el posible costo de pérdida de la categoría analizada.

Figura 11. *P-value para distribución de fraude externo*



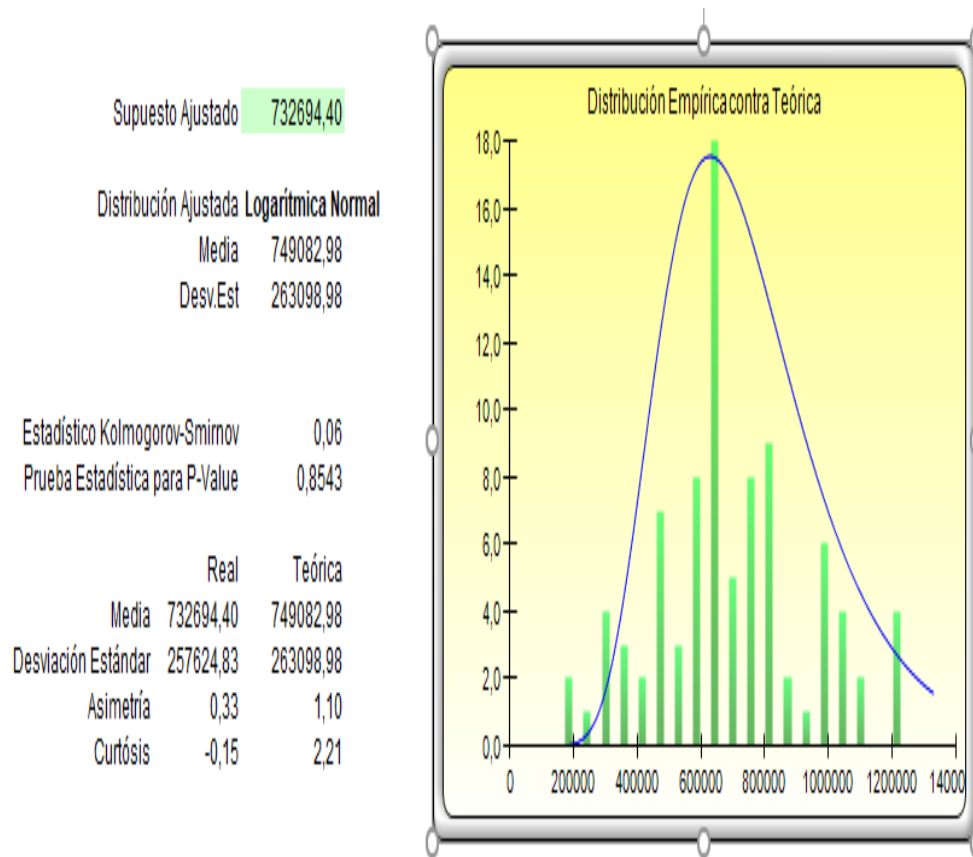
Los resultados obtenidos a partir del ajuste de distribución evidenciado en la Figura 10, permitieron demostrar que los registros se pueden ajustar para el modelo estadístico de pérdidas agregadas con una distribución Lognormal, pues su P-value es >0.5 , es decir 0.8543

La Figura 11, representa la distribución ajustada a la distribución Lognormal a la que se ajustó la distribución de severidad para la categoría fraude externo.

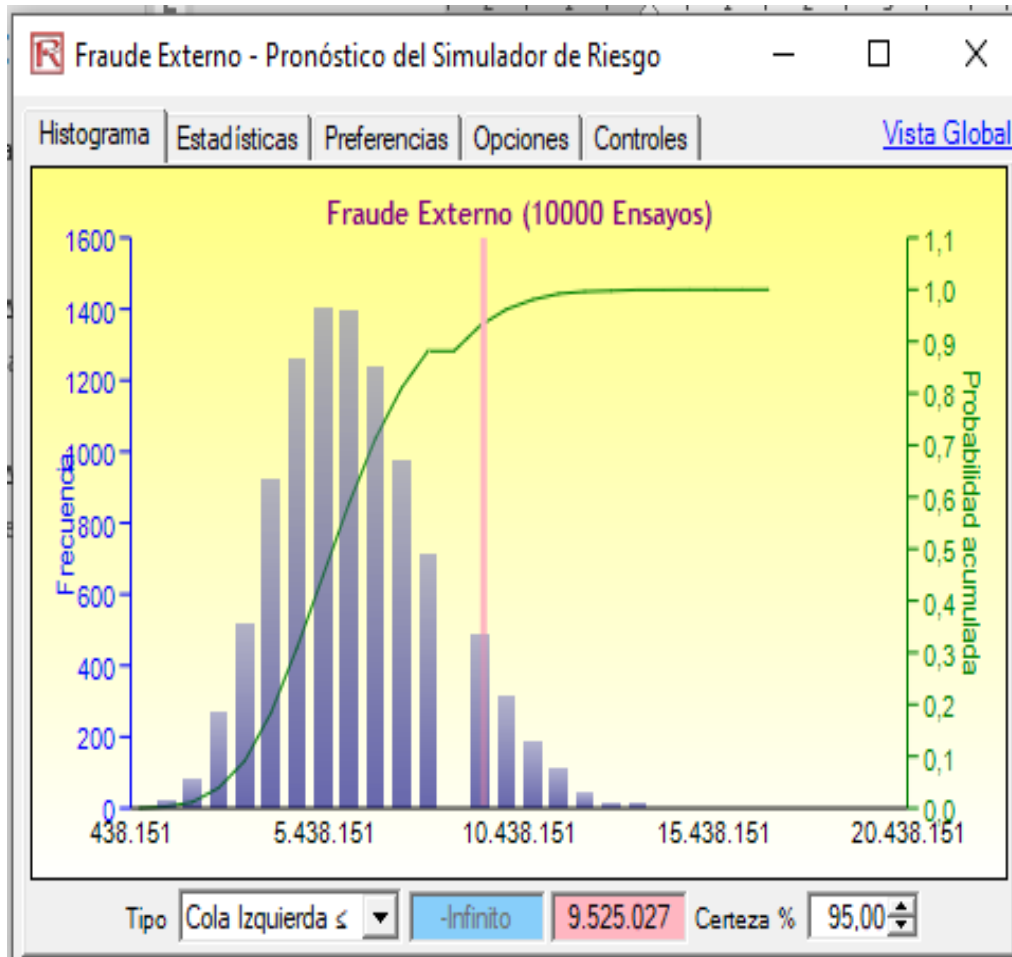
De igual manera, se establecieron otros parámetros estadísticos que pudieron ser analizados como la curtosis, la asimetría, y la desviación estándar.

Los estadísticos ya mencionados, sino fueron variables del modelo directamente sirvieron para establecer una caracterización cuantitativa de la serie de datos para la variable fraude externo.

Figura 12. Distribución de datos de severidad ajustada a la distribución Lognormal para fraude externo



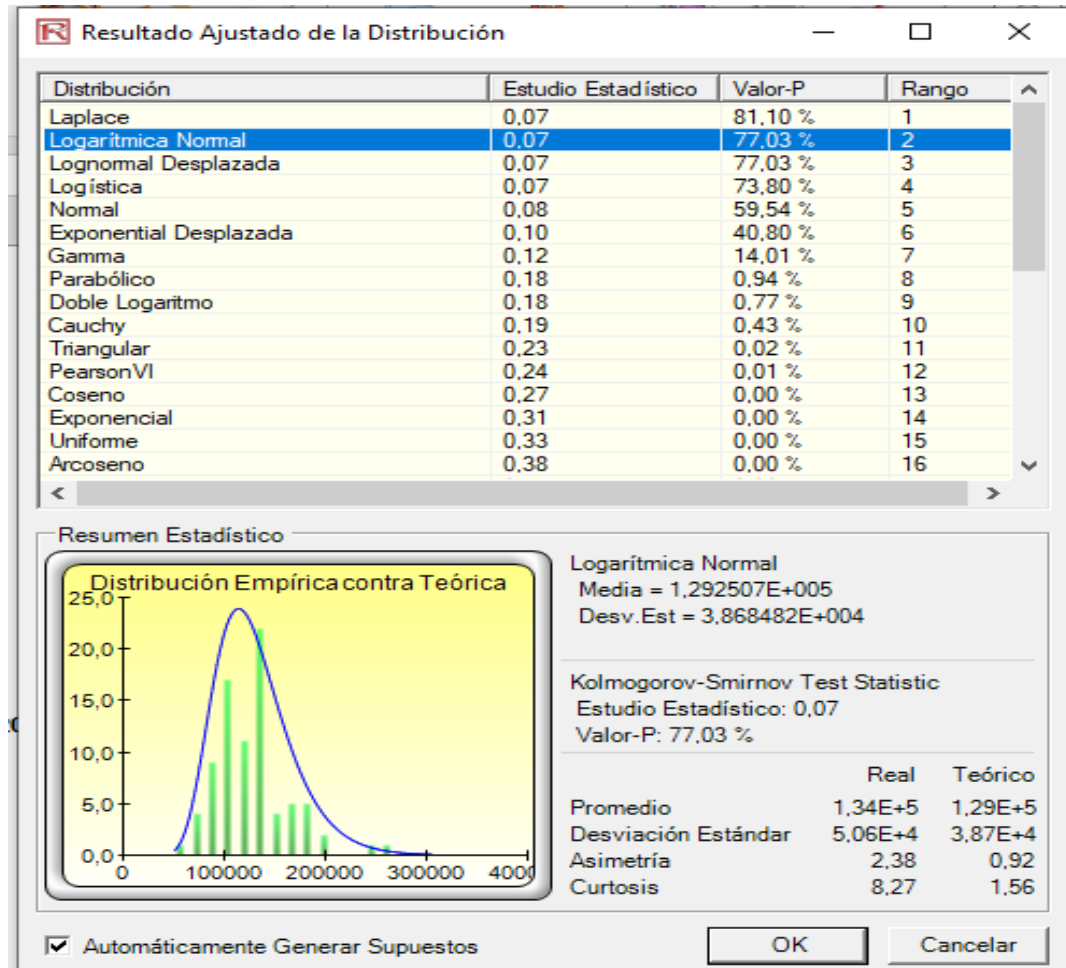
Así mismo, arrojó un supuesto ajustado a la media real de los datos que sirvió para alimentar las convoluciones del modelo. El cual fue de 732694,40.

Figura 13. Simulación de categoría fraude externo

La Figura 12, refleja los resultados obtenidos de la simulación para la categoría fraude externo que, a 10000 iteraciones, dio como resultado para el OpVar una aproximación del valor en riesgo de \$9.525. 027.

5.7.3 Ajuste de Distribución de Severidad de la Categoría Manejo de Procesos

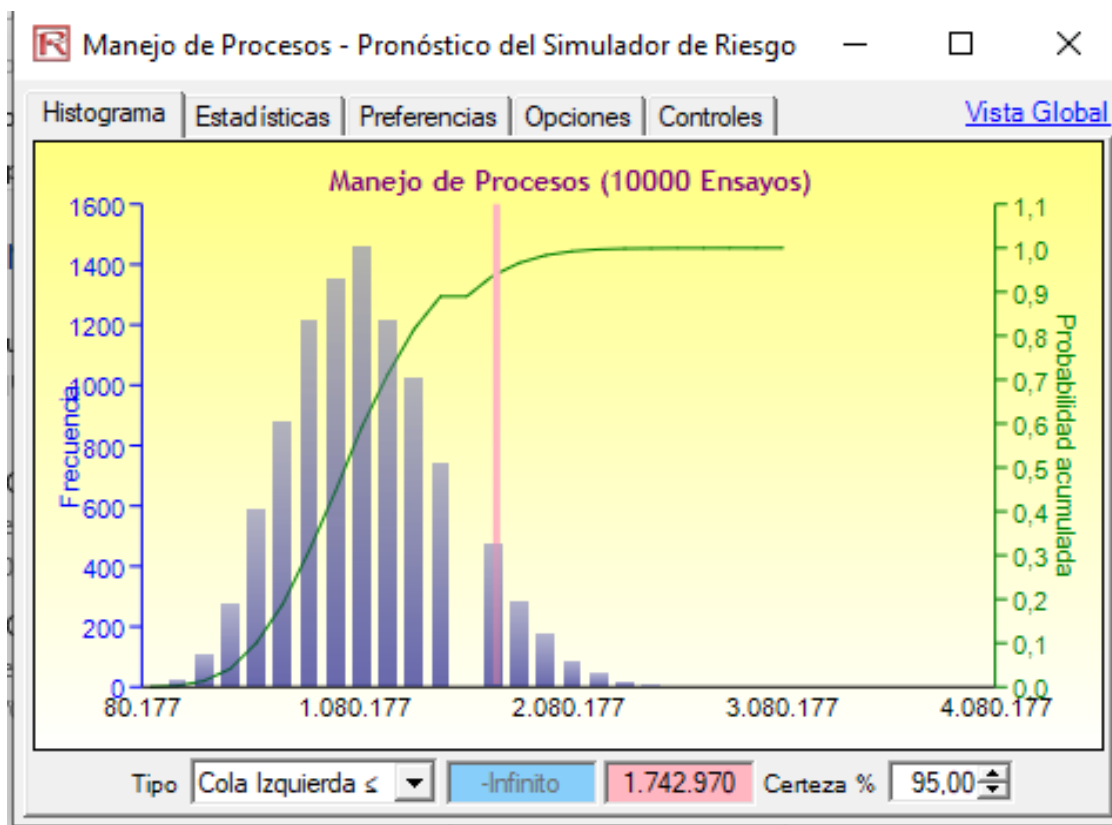
En la Figura 13, se puede observar que las distribuciones se ajustan de mejor manera a la distribución de severidad dada para la categoría manejo y ejecución de procesos.

Figura 14. *P-value para distribución Manejo y Ejecución de Procesos*

Los resultados obtenidos a partir del ajuste de distribución evidenciado en la Figura 13, demostraron que los registros se pueden ajustar para el modelo estadístico de pérdidas agregadas con una distribución Lognormal, pues su P-value es >0.5 , es decir 0.7703

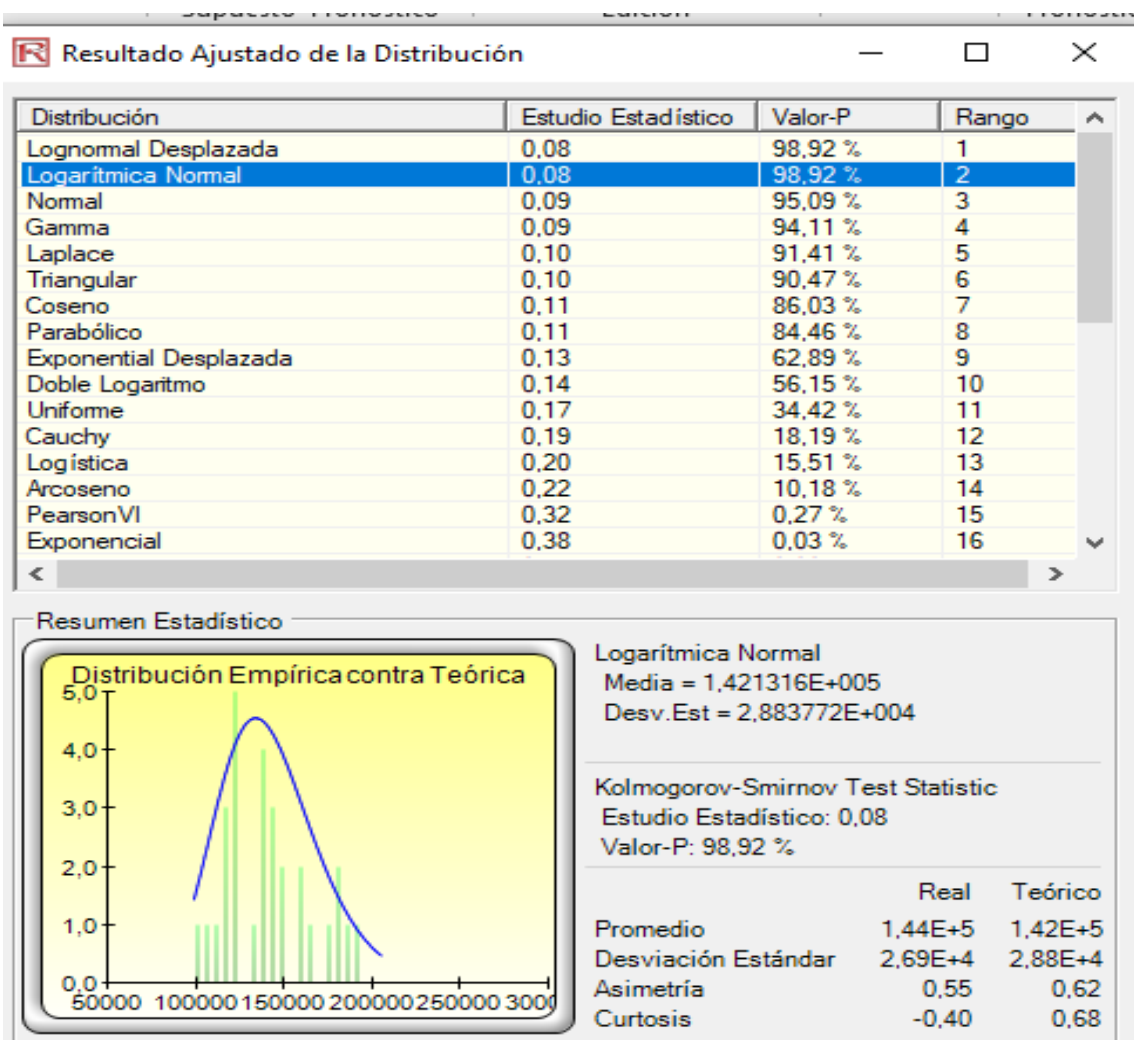
La Figura 14, representa la distribución ajustada a la distribución Lognormal a la que se ajustó la distribución de severidad para la categoría manejo y ejecución de procesos.

Así mismo, arrojó un supuesto ajustado a la media real de los datos que sirvió para alimentar las convoluciones del modelo. El cual tuvo un valor de 134074,59.

Figura 15. Simulación de categoría manejo y ejecución de procesos

La Figura 15, permitió determinar a partir de los resultados obtenidos de la simulación para la categoría manejo y ejecución de procesos que, a 10000 iteraciones, se logró obtener un OpVar aproximado de \$1.742. 970.

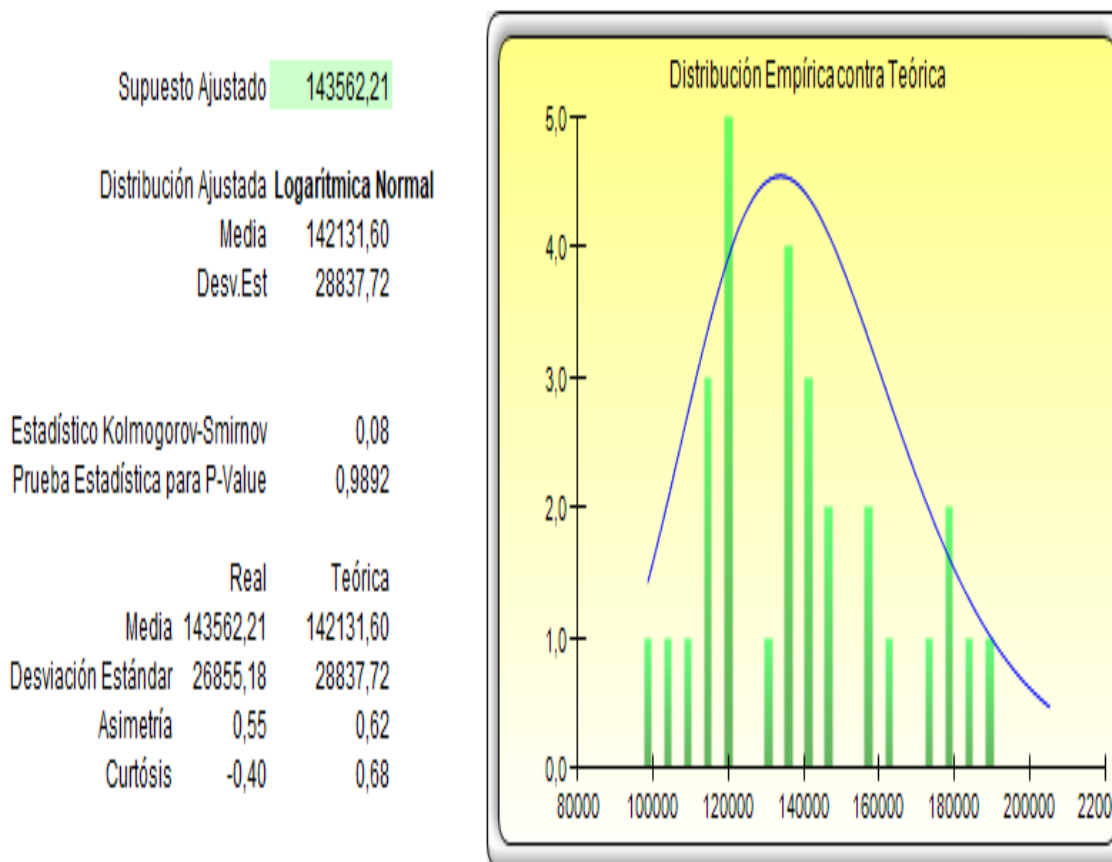
En la Figura 16, se puede observar que tipo de distribuciones se ajustaron mejor a la distribución de severidad dada para la categoría fallas en el sistema e interrupción del negocio.

Figura 16. P-value para distribución fallas en el sistema e interrupción del negocio

Los resultados obtenidos a partir del ajuste de distribución, permitieron demostrar a partir de la Figura 16 que los datos se pueden ajustar para el modelo estadístico de pérdidas agregadas con una distribución Lognormal, pues su P-value es >0.5 , es decir 0.9892

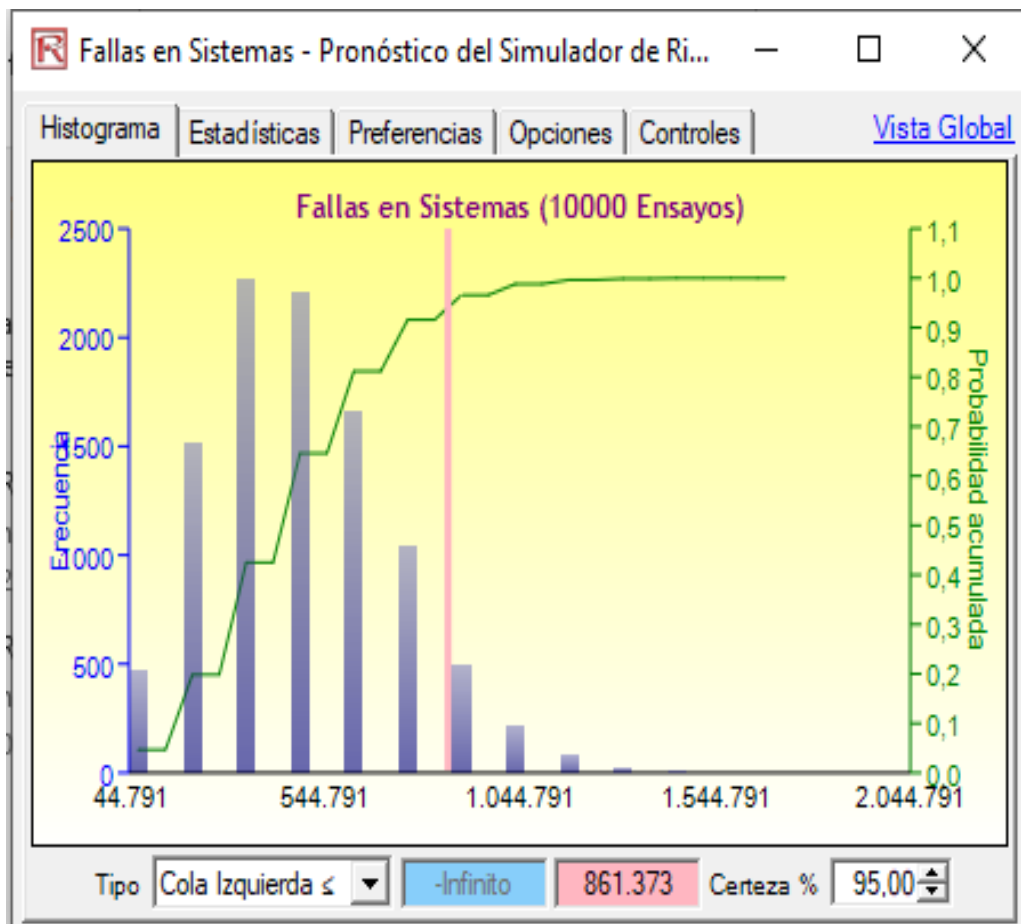
La Figura 17, representa la distribución ajustada a la distribución Lognormal a la que se ajustó la distribución de severidad para la categoría fraude externo.

Figura 17. Distribución de severidad ajustada a distribución Lognormal para fallas en el sistema e interrupción del negocio



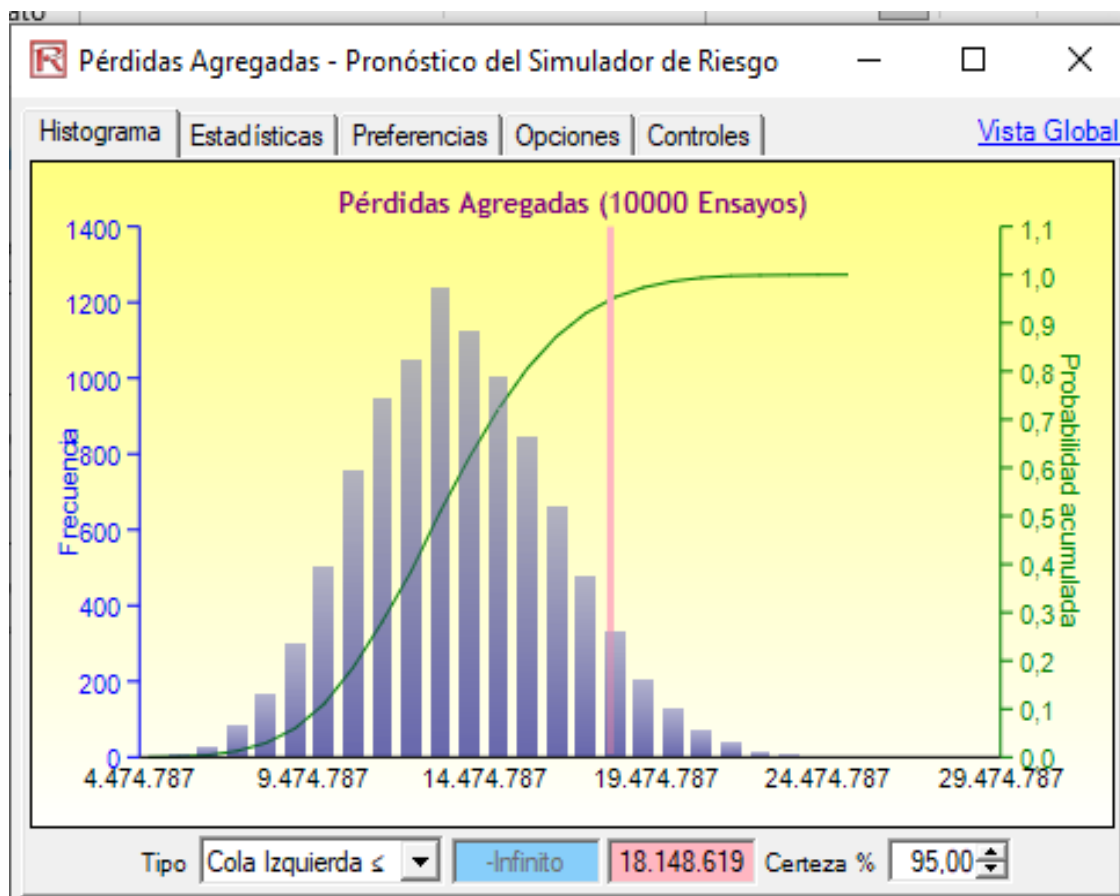
El ajuste realizado, arrojó un supuesto ajustado a la media real de los datos que sirvió para alimentar las convoluciones del modelo. El cual fue de 143562,21.

En la Figura 18, puede observarse la simulación para fallas en sistemas e interpretación del negocio, la línea rosada debe representa el OpVar o valor en riesgo que en promedio la sucursal bancaria puede estar sujeta a perder por eventos relacionados al riesgo operativo en esta categoría del negocio bancario.

Figura 18. Simulación de categoría fallas en sistemas e interrupción del negocio

La Figura 18, hizo posible establecer con base a los resultados obtenidos de la simulación para la categoría fallas en el sistema e interrupción del negocio que, a 10000 iteraciones, se logró estimar un OpVar aproximado de \$861.373.

La importancia que tiene la Figura 19 es que, sobre ella está simulado todo el riesgo operativo sobre el cual pudo estar sujeta la sucursal bancaria a incurrir si llegado el caso se hubiera dado algún evento de los relacionados en el modelo.

Figura 19. Simulación de pérdidas agregadas

Las pérdidas agregadas simuladas en la Figura 19, al valor en riesgo u OpVar que la sucursal bancaria podría estar expuesta a perder económicamente por caso que se presente de riesgo operacional durante el horizonte de tiempo de un año. La simulación reflejada combina posibles resultados de combinaciones de las distribuciones de frecuencia y severidad. El valor obtenido al percentil 95, equivale a \$18.148.619.

En la tabla 18, se estimaron los estadísticos del pronóstico resultante de la distribución de pérdidas agregadas.

Tabla 18. *Pronóstico del riesgo operativo resultante*

| Tabla estadística del pronóstico - Riesgo Operativo Sucursal Bancaria | | | | | |
|---|--------------------|----------------|----------------|--------------------|--------------------|
| Celda | Fallas en Sistemas | Fraude Externo | Fraude Interno | Manejo de Procesos | Pérdidas Agregadas |
| Nombre | \$E\$116 | \$E\$113 | \$E\$114 | \$E\$115 | \$E\$117 |
| Número de Intentos | 10.000 | 10.000 | 10.000 | 10.000 | 10.000 |
| Media (Pérdidas Esperadas) (\$) | 431.792 | 5.907.568 | 5.862.072 | 1.075.077 | 13.276.510 |
| Mediana (\$) | 430.687 | 5.861.555 | 5.875.521 | 1.072.597 | 13.144.345 |
| Desviación Standard (\$) | 248.721 | 2.077.736 | 1.914.115 | 377.475 | 2.858.165 |
| Percentil 25% (\$) | 287.124 | 4.396.166 | 4.569.850 | 804.448 | 11.270.983 |
| Percentil 75% (\$) | 574.249 | 7.326.944 | 7.181.192 | 1.340.746 | 15.178.343 |
| Precisión de Error 95% | 1,13% | 0,69% | 0,64% | 0,69% | 0,42% |
| Percentil 50% (\$) | 430.687 | 5.861.555 | 5.875.521 | 1.072.597 | 13.144.345 |
| Percentil 95% (Valor en Riesgo o Pérdida Catastrófica) (\$) | 861.373 | 9.525.027 | 9.139.699 | 1.742.970 | 18.148.619 |
| Percentil 99% (\$) | 1.148.498 | 10.990.416 | 10.445.370 | 2.011.119 | 20.276.331 |
| Pérdidas No Esperadas (\$) | 429.581 | 3.617.459 | 3.277.627 | 667.893 | 4.872.109 |

Nota: * resultados del modelo estadístico aplicado a las distribuciones de severidad y frecuencia de los posibles eventos de pérdidas en la sucursal bancaria.

Dentro de los estadísticos a resaltar en la Tabla 18, cabe mencionar la pérdida promedio para cada categoría entre las que sobresalen fraude interno con posibles pérdidas promedio de \$5.862.072 y fraude externo con posibles pérdidas promedio de \$5.907.568.

Otra inferencia importante a realizar sobre los estadísticos expuestos, es sobre la precisión del error al 95%. Lo anterior significa que, tal precisión debe ser inferior al 5%, de lo contrario debería aumentarse el tamaño de la muestra de la distribución simulada. Para todas las distribuciones de datos proporcionados por los expertos, la precisión del error fue menor o igual a 1,13% lo que validó la disciplina de la simulación ejecutada.

6. Conclusiones

Las inferencias realizadas sobre los enfoques ascendentes de Redes Bayesianas y Distribuciones de Pérdidas de manera avanzada para la cuantificación del riesgo operacional en una entidad bancaria de la ciudad de Bucaramanga, se presentan a continuación.

Se eligió la línea de negocio de Banca Minorista por ser la de mayor facilidad en cuanto a consulta de información y ubicación de expertos para implementar los modelos desarrollados.

En temas como el analizado en el presente proyecto, los juicios de expertos y experiencia de profesionales en el campo, resultó ser una manera viable y validada para conseguir la información que alimentaría los modelos estadísticos, tanto el causal como el desarrollado para cuantificar el OpVar o valor en riesgo.

Para la entidad bancaria que estuvo sujeta a la aplicación de la metodología propuesta, se evidenció que el primero de los enfoques descritos le permitió estructurar de manera dinámica, como estimar de forma probabilística los riesgos a los que puede estar expuesta si un conjunto de interrelaciones de posibles eventos de pérdidas se da bajo unas probabilidades subjetivas incorporadas al modelo de Red Bayesiana para cada categoría de pérdida.

El seguimiento de los especialistas en el tema resultó ser de gran importancia al momento de interpretar y validar los resultados de acuerdo a su experiencia, y la realidad del sistema financiero colombiano. Si bien fueron profesionales con experiencia teórica, también colocaron a disposición el conocimiento de los procesos, lo cual representó información oportuna para el análisis.

El desarrollo de la tesis permitió conocer de manera directa, que en los últimos años el sistema financiero colombiano se ha venido apegando a las recomendaciones dadas por el

Comité de Basilea en cuanto a la supervisión de los procesos y procedimientos dados al interior de cada institución, siendo la guía para el caso colombiano el Sistema de Administración del Riesgo Operacional (SARO).

7. Recomendaciones

Dado que la temática de estimar el RO en las instituciones financieras no es un tema muy antiguo, últimamente si ha tenido un impulso dentro de los bancos a nivel mundial por la importancia que tiene para ellos el controlar los riesgos asociados a cada actividad del negocio bancario que cada día se vuelven más complejas. Es por esto, que se requiere para mejores aplicaciones del tipo de riesgo analizado, se disponga de datos históricos o se considere la creación de bancos de datos para implementar metodologías necesitadas de datos actualizados constantemente.

Si bien es entendible la confidencialidad de la información para cada entidad financiera, se hace necesario una alianza empresa-academia para de manera conjunta poder desarrollar aplicaciones de manera simulada con datos si cabe la posibilidad de carácter aproximados a los reales para que la brecha experiencia académica-experiencia laboral no sean tan distantes.

Se ha vuelto indispensable, y lo seguirá siendo, que los colaboradores de las entidades cada día se integren en una cultura de gestión del riesgo para que de tal manera al conocer más los procesos puedan ser expertos en el área y así mismo poder proporcionar información sin gran nivel de sesgo para que los resultados sean razonables con el contexto objeto de estudio

Referencias

- [1] F. E. Posada Espinal, «Repositorio Universidad Nacional de Colombia,» 28 Noviembre 2011. [En línea]. Available: <https://repositorio.unal.edu.co/handle/unal/11227>.
- [2] Banco de Pagos Internacionales, «Bis,» Enero 2001. [En línea]. Available: Nuevo Acuerdo de Capitales de Basilea 2004.
- [3] A. J. Soto Quintana, S. Marcial y M. R. Valente Martinez, «Gestion del riesgo operacional en la banca universal venezolana,» *Revista Venezolana de Gerencia*, vol. 14, n° 45, pp. 96-109, 2009.
- [4] G. Dávila Aragón , «Repositorio Instituto Tecnológico y de Estudios Superiores de Monterrey,» Abril 2014. [En línea]. Available: <https://repositorio.tec.mx/bitstream/handle/11285/628895/33068001114322.pdf?sequence=1&isAllowed=y>.
- [5] J. A. Peña Salazar, «Reporitorio Institucional UNMG,» 2014. [En línea]. Available: <https://repository.unimilitar.edu.co/bitstream/handle/10654/13199/Ensayo%20de%20Grado%20-%20Final%2020Ene15.pdf?sequence=1&isAllowed=y>.
- [6] J. López Puga, «Cómo Construir y Validar Redes Bayesianas con Netica,» *Revista Electrónica de Metodología Aplicada*, vol. 17, n° 1, pp. 1-17, 2012.

- [7] M. d. C. Chávez, R. Grau y M. M. García, «Método para construir redes bayesianas,» *REVISTA FACULTAD DE INGENIERÍA UNIVERSIDAD DE ANTIOQUIA*, n° 19, pp. 76-84, 2016.
- [8] L. O. Mesa Páez, M. Rivera Lozano y J. A. Romero Davila, «Laboratorio de modelamiento y simulacion Universidad del Rosario,» Febrero 2011. [En línea]. Available: https://www.urosario.edu.co/Administracion/documentos/investigacion/laboratorio/miller_2_2.pdf.
- [9] . D. . D. Wackerly, W. Mendenhall III y R. . L. Scheaffer, de *Estadística matemática con aplicaciones*, Séptima ed., México, CENGAGE Learning, 2010, pp. 52-53.
- [10] G. SHAFER y J. PEARL, «Readings in,» San Francisco, Morgan Kaufmann Publishers Inc, 1990, pp. 345-352.
- [11] J. PEARL, «CAUSALITY:Models, Reasoning, and Inference,» Los Angeles, CAMBRIDGE UNIVERSITY PRESS, 2000, pp. CAP.1,5,7.
- [12] D. Geiger, N. Friedman y M. Goldszmidt , «Bayesian network classifiers Machine Learning 29,» *Springer LINK*, pp. 131-167, 1997.
- [13] C. Alexander, «Operational Risk: Regulation, Analysis and Management,» Prentice Hall, 2003.
- [14] M. Rivera Lozano, «Laboratorio de modelamiento y simulación Universidad del Rosario,» Febrero 2011. [En línea]. Available: https://www.urosario.edu.co/Administracion/documentos/investigacion/laboratorio/miller_2_3.pdf.

- [15] L. E. Sucar y M. Martínez Arroyo, «Departamento de lenguaje y sistemas informaticos Universidad de Sevilla,» 2002. [En línea]. Available: <http://www.lsi.us.es/iberamia2002/confman/SUBMISSIONS/288-uirusmaiqu.pdf>.
- [16] P. . F. Hernández Leal, «Repositorio Institucional INAOE,» [En línea]. Available: <https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/687/1/HernandezLPF.pdf>.
- [17] K. E. ARIAS REYES, M. R. FÁREZ SANCHEZ y L. CALDERON PERALTA, «Repositorio Institucional Universidad del Azuay,» 2007. [En línea]. Available: <http://dspace.uazuay.edu.ec/handle/datos/2283?locale=en>.
- [18] S. Russell y P. Norvig, de *INTELIGENCIA ARTIFICIAL. UN ENFOQUE MODERNO*, Segunda ed., Madrid, Prentice Hall, 2004, pp. 577-578.
- [19] J. D. Tardós, «Departamento de Informática e Ingeniería de Sistemas,» 9 Septiembre 2012. [En línea]. Available: http://webdiis.unizar.es/~jangelb/IA-30223/L12_Redес_Bayesianas.pptx. [Último acceso: 18 Octubre 2020].
- [20] D. d. L. y. C. d. I. C. U. d. Málaga, «Departamento de Lenguajes y Ciencias de la Computación Universidad de Málaga,» 17 Agosto 2009. [En línea]. Available: <http://www.lcc.uma.es/~eva/aic/Redes%20Bayesianas.pdf>. [Último acceso: 18 Octubre 2020].
- [21] L. E. Sucar, «INSTITUTO NACIONAL DE ASTROFÍSICA, ÓPTICA Y ELECTRÓNICA,» 2002. [En línea]. Available: <https://ccc.inaoep.mx/~esucar/Clases-mgp/caprb.pdf>.

- [22] C. Lorena Corso y F. Gibellini, «CACIC 2011 - XVII CONGRESO ARGENTINO DE CIENCIAS DE LA COMPUTACIÓN,» de *Aplicación de Redes bayesianas usando Weka*, Buenos Aires, 2011.
- [23] L. A. Rey, «REVISTAdigital INESEM,» 30 Noviembre 2017. [En línea]. Available: <https://revistadigital.inesem.es/gestion-empresarial/riesgo-financiero/>.
- [24] S. F. d. Colombia, «SFC,» [En línea]. Available: <https://www.superfinanciera.gov.co/jsp/Glosario/user/main/letra/B/f/0/c/0>. [Último acceso: 17 Agosto 2020].
- [25] I. López Domínguez , «EXPANSION.com,» 14 Agosto 2020. [En línea]. Available: <https://www.expansion.com/diccionario-economico/entidad-financiera.html#:~:text=En%20general%2C%20cualquier%20entidad%20que,la%20modalidad%2C%20a%20su%20clientela.&text=En%20definitiva%2C%20las%20entidades%20que,Valores%20y%20%20C3%81rea%20de%20Seguros..>
- [26] G. Heinrich, «Banco Internacional de Pagos,» 2006. [En línea]. Available: https://www.bis.org/repofficepubl/heinrich_riesgo_operacional_a.pdf.
- [27] J. A. Miccolis y S. Shah, «COLLEGE OF BUSINESS Illinois States University,» 11 Abril 2006. [En línea]. Available: <https://business.illinoisstate.edu/katie/industry/presentations/Evan%20Busman%20-%20Tillinghast%20ERM%20Presentation.pdf>.
- [28] L. M. Pinto Gaviria y A. Leyva Lemarie, «Administración del riesgo operacional en Colombia Estado de la implementación del SARO en el sector bancario,» *AD-MINISTER Universidad EAFIT*, n° 12, pp. 89-106, 2008.

- [29] SUPERINTENDENCIA FINANCIERA DE COLOMBIA, «promotec,» 22 Diciembre 2006. [En línea]. Available: https://www.promotec.com.co/descargables/pdf/normativas/ce048_06.pdf.
- [30] ASOBANCARIA, «ASOBANCARIA,» 15 Agosto 2020. [En línea]. Available: <https://www.asobancaria.com/capacitaciones-saro/>.
- [31] BBVA, «BBVA,» 2012. [En línea]. Available: [https://accionistaseinversores.bbva.com/microsites/bbva2012/es/Gestiondelriesgo/Riesgooperacional.html#:~:text=El%20riesgo%20operacional%20es%20inherente,comerciales%2C%20desastres%2C%20proveedores\)..](https://accionistaseinversores.bbva.com/microsites/bbva2012/es/Gestiondelriesgo/Riesgooperacional.html#:~:text=El%20riesgo%20operacional%20es%20inherente,comerciales%2C%20desastres%2C%20proveedores)..)
- [32] J. F. Martínez-Sánchez y F. Venegas-Martínez, «Riesgo operacional en la banca trasnacional:», *Ensayos Revista de Economía*, vol. 32, n° 1, pp. 31-72, 2013.
- [33] P. Giudici y A. Bilotta, «Modelling Operational Losses: A Bayesian Approach,» *Quality and Reliability Engineering International*, vol. 20, n° 5, pp. 407-417, 2004.
- [34] G. Dávila Aragón y F. Ortiz Arango , «Cálculo del Valor en Riesgo Operacional de una Empresa Aseguradora Mediante Redes Bayesianas,» *REVISTA DE METODOS CUANTITATIVOS PARA LA ECONOMÍA Y LA EMPRESA*, pp. 30-55, 2019.
- [35] R. G. Cowell, R. J. Verrall y Y. K. Yoon, «Modeling Operational Risk With Bayesian Networks,» *Online library Wiley*, vol. 74, n° 4, pp. 795-827, 2007.
- [36] J. . F. Martínez Sánchez y F. Venegas Martínez, «Riesgo operacional en el proceso de pago del Procampo Un enfoque bayesiano,» *Contaduría y Administración*, vol. 58, n° 2, pp. 221-259, 2013.

- [37] G. Dávila-Aragón, S. Rivas-Aceves y F. Ortiz-Arango, «Operational Risk Measured by Bayesian Networks with a Poisson-Gamma Joint Distribution in a Financial Firm,» *Revista mexicana de economía y finanzas*, vol. 12, n° 4, pp. 351-363, 2013.
- [38] A. C. González Martínez, N. A. Bautista Hernández, M. A. Ramírez Guerrero y J. Franco, «Polux,» Junio 2015. [En línea]. Available: <http://polux.unipiloto.edu.co:8080/00002520.pdf>.
- [39] V. Aquaro, M. Bardoscia, R. Bellotti, A. Consiglio, F. De Carlo y G. Ferri, «A Bayesian Networks approach to Operational Risk,» *Physica A: Statistical Mechanics and its Applications*, vol. 389, n° 8, pp. 1721-1728, 2010.
- [40] C. Alexander, «SSRN,» 6 Diciembre 2000. [En línea]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=248148. [Último acceso: 18 Octubre 2020].
- [41] J. F. Martínez Sánchez, M. T. Martínez Palacios y F. Venegas Martínez, «An analysis on operational risk in international banking: A Bayesian approach (2007–2011),» *Estudios Gerenciales*, vol. 32, n° 140, pp. 208-220, 2016.
- [42] M. Castillo y Á. Mendoza, «DISEÑO DE UNA METODOLOGÍA PARA LA IDENTIFICACIÓN Y LA MEDICIÓN DEL RIESGO OPERATIVO EN INSTITUCIONES FINANCIERAS,» *REVISTA DE INGENIERIA UNIVERSIDAD DE LOS ANDES*, pp. 45-52, 2004.
- [43] R. Hernández Sampieri, C. Fernández Collado y P. Baptista Lucio, «METODLOGÍA DE LA INVESTIGACIÓN,» México, McGraw-Hill, 2006, p. 102.

- [44] L. C. Franco Arbélaez, «Repositorio EAFIT,» 2009. [En línea]. Available: https://repository.eafit.edu.co/bitstream/handle/10784/135/LuisCeferino_FrancoArbelaez_2010.pdf?sequence=3.

Apéndices

Apéndice A. Probabilidades condicionales para fraude interno parte 1

Hugin Lite 8.9

File Data Edit View Network Options Windows Wizards Help

Class: Fraudenterno

| | | Mala | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|-----------------|------|-------|-------|------|-------|------|------|-------|-------|------|-------|------|-------|-------|-------|------|-------|-------|------|-------|-------|------|-------|-------|------|
| | | Si | | | | | | | | | | | | No | | | | | | | | | | | | |
| | | Si | | | | | | No | | | | | | Si | | | | | | No | | | | | | |
| Supervision | Nivel_restri... | Bajo | | Medio | | Alto | | Bajo | | Medio | | Alto | | Bajo | | Medio | | Alto | | Bajo | | Medio | | Alto | | |
| Entrega_Se... | | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja |
| Nivel_1 | | 0.6 | 0.5 | 0.55 | 0.55 | 0.65 | 0.7 | 0.65 | 0.7 | 0.72 | 0.85 | 0.85 | 0.75 | 0.83 | 0.089 | 0.89 | 0.9 | 0.91 | 0.92 | 0.79 | 0.82 | 0.84 | 0.8 | 0.85 | 0.87 | 0.82 |
| Nivel_2 | | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.2 | 0.25 | 0.25 | 0.25 | 0.1 | 0.05 | 0.15 | 0.07 | 0.06 | 0.07 | 0.08 | 0.07 | 0.07 | 0.06 | 0.07 | 0.08 | 0.05 | 0.07 | 0.08 | 0.07 |
| Nivel_3 | | 0.1 | 0.15 | 0.15 | 0.1 | 0.05 | 0.05 | 0.1 | 0.05 | 0.03 | 0.03 | 0.05 | 0.05 | 0.05 | 0.025 | 0.02 | 0.01 | 0.01 | 0.005 | 0.05 | 0.06 | 0.07 | 0.05 | 0.06 | 0.025 | 0.05 |
| Nivel_4 | | 0.05 | 0.05 | 0.05 | 0.05 | 0.05 | 0 | 0 | 0 | 0.02 | 0.05 | 0.05 | 0.05 | 0.025 | 0.02 | 0.01 | 0.01 | 0.005 | 0.05 | 0.03 | 0.01 | 0.05 | 0.02 | 0.025 | 0.03 | |
| Nivel_5 | | 0 | 0.05 | 0 | 0.05 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.05 | 0.02 | 0 | 0.05 | 0 | 0 | 0.03 | |

Apéndice B. Probabilidades condicionales para fraude interno parte 2

Hugin Lite 8.9

File Data Edit View Network Options Windows Wizards Help

Class: Fraudenterno

| | | Mala | | | | | | | | | | | | Regular | | | | | | | | | | | | |
|---------------|-----------------|-------|------|-------|-------|------|------|-------|------|-------|-------|-------|-------|---------|------|-------|-------|------|------|-------|------|-------|-------|-------|-------|------|
| | | No | | | | | | | | | | | | Si | | | | | | | | | | | | |
| | | Si | | | | | | No | | | | | | Si | | | | | | No | | | | | | |
| Supervision | Nivel_restri... | Bajo | | Medio | | Alto | | Bajo | | Medio | | Alto | | Bajo | | Medio | | Alto | | Bajo | | Medio | | Alto | | |
| Entrega_Se... | | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | |
| Nivel_1 | | 0.83 | 0.85 | 0.75 | 0.8 | 0.82 | 0.88 | 0.9 | 0.91 | 0.85 | 0.87 | 0.9 | 0.78 | 0.86 | 0.89 | 0.79 | 0.85 | 0.89 | 0.79 | 0.87 | 0.89 | 0.78 | 0.8 | 0.81 | 0.83 | 0.84 |
| Nivel_2 | | 0.08 | 0.09 | 0.1 | 0.08 | 0.09 | 0.08 | 0.08 | 0.07 | 0.1 | 0.08 | 0.09 | 0.08 | 0.09 | 0.09 | 0.09 | 0.09 | 0.09 | 0.15 | 0.09 | 0.08 | 0.08 | 0.08 | 0.1 | 0.07 | 0.08 |
| Nivel_3 | | 0.06 | 0.03 | 0.08 | 0.07 | 0.08 | 0.03 | 0.01 | 0.01 | 0.025 | 0.02 | 0.005 | 0.07 | 0.04 | 0.02 | 0.07 | 0.04 | 0.02 | 0.05 | 0.03 | 0.03 | 0.06 | 0.07 | 0.08 | 0.05 | 0.06 |
| Nivel_4 | | 0.015 | 0.03 | 0.035 | 0.025 | 0.01 | 0.01 | 0.01 | 0.01 | 0.025 | 0.02 | 0.005 | 0.035 | 0.005 | 0 | 0.025 | 0.02 | 0 | 0.01 | 0.01 | 0 | 0.05 | 0.03 | 0.01 | 0.025 | 0.01 |
| Nivel_5 | | 0.015 | 0 | 0.035 | 0.025 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 | 0.035 | 0.005 | 0 | 0.025 | 0 | 0 | 0 | 0 | 0.03 | 0.02 | 0 | 0.025 | 0.01 | |

Apéndice C. Probabilidades condicionales para fraude interno parte 3

| Fraude Interno | | Buena | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|--|-------|-------|-------|------|------|-------|------|------|-------|------|------|-------|-------|------|-------|------|-------|-------|------|-------|-------|------|------|-------|------|
| Calidad_Per... | | Buena | | | | | | | | | | | | | | | | | | | | | | | | |
| Manejo_se... | | No | | | | | | | | | | | | | | | | | | | | | | | | |
| Supervision | | No | | | | | Si | | | | | No | | | | | | | | | | | | | | |
| Nivel_restri... | | Medio | | | Alto | | Bajo | | | Medio | | | Alto | | Bajo | | | Medio | | Alto | | Bajo | | | | |
| Entrega_Se... | | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta |
| Nivel_1 | | 0.85 | 0.84 | 0.86 | 0.88 | 0.83 | 0.85 | 0.88 | 0.84 | 0.87 | 0.89 | 0.81 | 0.82 | 0.85 | 0.78 | 0.82 | 0.85 | 0.82 | 0.85 | 0.87 | 0.84 | 0.87 | 0.89 | 0.78 | 0.8 | 0.87 |
| Nivel_2 | | 0.09 | 0.06 | 0.07 | 0.09 | 0.06 | 0.07 | 0.09 | 0.08 | 0.09 | 0.09 | 0.08 | 0.09 | 0.1 | 0.1 | 0.15 | 0.09 | 0.08 | 0.09 | 0.1 | 0.06 | 0.07 | 0.08 | 0.08 | 0.1 | 0.11 |
| Nivel_3 | | 0.05 | 0.05 | 0.04 | 0.03 | 0.05 | 0.04 | 0.02 | 0.06 | 0.02 | 0.02 | 0.07 | 0.07 | 0.025 | 0.06 | 0.02 | 0.04 | 0.05 | 0.04 | 0.02 | 0.05 | 0.06 | 0.03 | 0.06 | 0.04 | 0.02 |
| Nivel_4 | | 0.01 | 0.025 | 0.015 | 0 | 0.03 | 0.02 | 0.01 | 0.02 | 0.02 | 0 | 0.04 | 0.02 | 0.025 | 0.03 | 0.01 | 0.02 | 0.025 | 0.02 | 0.02 | 0.025 | 0 | 0 | 0.05 | 0.03 | 0 |
| Nivel_5 | | 0 | 0.025 | 0.015 | 0 | 0.03 | 0.02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.03 | 0 | 0 | 0.025 | 0.02 | 0 | 0.025 | 0 | 0 | 0.03 | 0.03 | 0 |

Apéndice D. Probabilidades condicionales para fraude interno parte 4

| Fraude Interno | | Buena | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|--|-------|-------|------|------|-------|------|------|-------|-------|------|-------|------|------|-------|------|------|-------|------|-------|-------|-------|------|-------|------|------|
| Calidad_Per... | | Buena | | | | | | | | | | | | | | | | | | | | | | | | |
| Manejo_se... | | Si | | | | | | | | | | | | | | | | | | | | | | | | |
| Supervision | | Si | | | | | No | | | | | Si | | | | | No | | | | | | | | | |
| Nivel_restri... | | Medio | | | Alto | | Bajo | | | Medio | | | Alto | | Bajo | | | Medio | | Alto | | Bajo | | | | |
| Entrega_Se... | | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja |
| Nivel_1 | | 0.79 | 0.84 | 0.88 | 0.8 | 0.82 | 0.85 | 0.89 | 0.87 | 0.89 | 0.87 | 0.88 | 0.88 | 0.83 | 0.85 | 0.87 | 0.84 | 0.85 | 0.87 | 0.83 | 0.85 | 0.086 | 0.83 | 0.85 | 0.87 | 0.78 |
| Nivel_2 | | 0.09 | 0.09 | 0.07 | 0.08 | 0.09 | 0.09 | 0.07 | 0.08 | 0.09 | 0.07 | 0.08 | 0.09 | 0.07 | 0.08 | 0.09 | 0.06 | 0.06 | 0.08 | 0.07 | 0.08 | 0.07 | 0.08 | 0.09 | 0.09 | 0.08 |
| Nivel_3 | | 0.07 | 0.06 | 0.05 | 0.06 | 0.05 | 0.06 | 0.02 | 0.03 | 0.01 | 0.04 | 0.04 | 0.03 | 0.05 | 0.04 | 0.04 | 0.04 | 0.07 | 0.05 | 0.05 | 0.04 | 0.06 | 0.07 | 0.06 | 0.04 | 0.08 |
| Nivel_4 | | 0.025 | 0.01 | 0 | 0.04 | 0.04 | 0 | 0.01 | 0.02 | 0.01 | 0.02 | 0 | 0 | 0.05 | 0.03 | 0 | 0.03 | 0.02 | 0 | 0.025 | 0.015 | 0.01 | 0.02 | 0 | 0 | 0.03 |
| Nivel_5 | | 0.025 | 0 | 0 | 0.02 | 0 | 0 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.03 | 0 | 0 | 0.025 | 0.015 | 0 | 0 | 0 | 0 | 0.03 |

Apéndice E. Probabilidades condicionales para fraude interno parte 5

| Fraude Interno | | Buena | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|--|-------|------|-------|------|------|-------|------|------|-------|------|-------|-------|-------|------|-------|------|-------|-------|------|------|-------|------|------|-------|------|
| Calidad_Per... | | Buena | | | | | | | | | | | | | | | | | | | | | | | | |
| Manejo_se... | | No | | | | | | | | | | | | | | | | | | | | | | | | |
| Supervision | | No | | | | | Si | | | | | No | | | | | | | | | | | | | | |
| Nivel_restri... | | Medio | | | Alto | | Bajo | | | Medio | | | Alto | | Bajo | | | Medio | | Alto | | | | | | |
| Entrega_Se... | | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta | Baja | Media | Alta |
| Nivel_1 | | 0.89 | 0.87 | 0.88 | 0.88 | 0.83 | 0.85 | 0.87 | 0.84 | 0.85 | 0.87 | 0.83 | 0.85 | 0.086 | 0.83 | 0.85 | 0.87 | 0.78 | 0.84 | 0.85 | 0.82 | 0.84 | 0.86 | 0.81 | 0.82 | 0.85 |
| Nivel_2 | | 0.09 | 0.07 | 0.08 | 0.09 | 0.07 | 0.08 | 0.09 | 0.06 | 0.06 | 0.08 | 0.07 | 0.08 | 0.07 | 0.08 | 0.09 | 0.09 | 0.08 | 0.08 | 0.09 | 0.08 | 0.08 | 0.09 | 0.12 | 0.14 | 0.14 |
| Nivel_3 | | 0.01 | 0.04 | 0.04 | 0.03 | 0.05 | 0.04 | 0.04 | 0.04 | 0.07 | 0.05 | 0.05 | 0.04 | 0.06 | 0.07 | 0.06 | 0.04 | 0.08 | 0.04 | 0.06 | 0.07 | 0.07 | 0.03 | 0.06 | 0.04 | 0.01 |
| Nivel_4 | | 0.01 | 0.02 | 0 | 0 | 0.05 | 0.03 | 0 | 0.03 | 0.02 | 0 | 0.025 | 0.015 | 0.01 | 0.02 | 0 | 0 | 0.03 | 0.02 | 0 | 0.03 | 0.01 | 0.02 | 0.01 | 0 | 0 |
| Nivel_5 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.03 | 0 | 0 | 0.025 | 0.015 | 0 | 0 | 0 | 0 | 0.03 | 0.02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Apéndice F. Probabilidades condicionales para fallas en sistema e interrupción del negocio

Hugin Lite 8.9

File Data Edit View Network Options Windows Wizards Help

Class: Fallos_sistema

| Disponibil... | Bajo | | | | | | Esporadico | | | | | | Constante | | | | | |
|---------------|------|-------|------|------|-------|------|------------|-------|------|------|-------|------|-----------|-------|------|------|-------|------|
| | Si | | | No | | | Si | | | No | | | Si | | | No | | |
| Nivel_Cal... | Bajo | Medio | Alto | Bajo | Medio | Alto | Bajo | Medio | Alto | Bajo | Medio | Alto | Bajo | Medio | Alto | Bajo | Medio | Alto |
| Nivel_1 | 0.55 | 0.7 | 0.6 | 0.6 | 0.7 | 0.78 | 0.8 | 0.85 | 0.65 | 0.76 | 0.85 | 0.65 | 0.75 | 0.75 | 0.75 | 0.6 | 0.7 | 0.75 |
| Nivel_2 | 0.15 | 0.15 | 0.2 | 0.1 | 0.1 | 0.15 | 0.08 | 0.1 | 0.2 | 0.1 | 0.05 | 0.1 | 0.1 | 0.15 | 0.15 | 0.1 | 0.15 | 0.15 |
| Nivel_3 | 0.15 | 0.15 | 0.1 | 0.1 | 0.1 | 0.07 | 0.07 | 0.05 | 0.15 | 0.1 | 0.05 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 |
| Nivel_4 | 0.1 | 0 | 0 | 0.1 | 0.05 | 0 | 0.05 | 0 | 0 | 0.03 | 0.05 | 0.1 | 0.05 | 0 | 0 | 0.1 | 0.05 | 0 |
| Nivel_5 | 0.05 | 0 | 0 | 0.1 | 0.05 | 0 | 0 | 0 | 0 | 0.03 | 0 | 0.05 | 0 | 0 | 0 | 0.1 | 0 | 0 |

Apéndice G. Probabilidades condicionales para fraude externo

Hugin Lite 8.9

File Data Edit View Network Options Windows Wizards Help

Class: Fraudeexterno

| Control_Su... | Bajo | | | Medio | | | Alto | | |
|---------------|------|-------|------|-------|-------|------|------|-------|------|
| | Bajo | Medio | Alto | Bajo | Medio | Alto | Bajo | Medio | Alto |
| Nivel_1 | 0.6 | 0.75 | 0.86 | 0.72 | 0.89 | 0.9 | 0.79 | 0.78 | 0.75 |
| Nivel_2 | 0.2 | 0.15 | 0.08 | 0.18 | 0.05 | 0.04 | 0.15 | 0.09 | 0.1 |

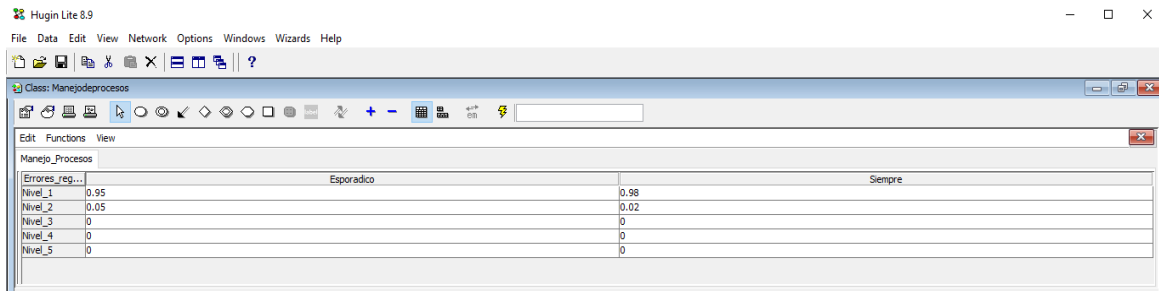
Apéndice H. Probabilidades condicionales para nodo calidad de personal

Hugin Lite 8.9

File Data Edit View Network Options Windows Wizards Help

Class: Fraudenterno

| Personal_A... | Bajo | | | | Medio | | | | Alto | | | |
|---------------|--------------------------|-----------------------|--------------------------|-----------------------|--------------------------|-----------------------|--------------------------|-----------------------|--------------------------|-----------------------|--------------------------|-----------------------|
| | No_presenta_antecedentes | Presenta_antecedentes | No_presenta_antecedentes | Presenta_antecedentes | No_presenta_antecedentes | Presenta_antecedentes | No_presenta_antecedentes | Presenta_antecedentes | No_presenta_antecedentes | Presenta_antecedentes | No_presenta_antecedentes | Presenta_antecedentes |
| Mala | 0.25 | 0.78 | 0.1 | 0.1 | 0.5 | 0.1 | 0.1 | 0.5 | 0.1 | 0.1 | 0.5 | 0.5 |
| Regular | 0.4 | 0.12 | 0.35 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 |
| Buena | 0.35 | 0.1 | 0.55 | 0.2 | 0.2 | 0.6 | 0.6 | 0.2 | 0.2 | 0.2 | 0.2 | 0.2 |

Apéndice I. Probabilidades condicionales para manejo y ejecución de procesos

The screenshot shows the Hugin Lite 8.9 interface. The main window displays a table titled 'Manejo_Procesos' with the following data:

| Errores_reg... | Esporadico | Siempre |
|----------------|------------|---------|
| Nivel_1 | 0.95 | 0.98 |
| Nivel_2 | 0.05 | 0.02 |
| Nivel_3 | 0 | 0 |
| Nivel_4 | 0 | 0 |
| Nivel_5 | 0 | 0 |